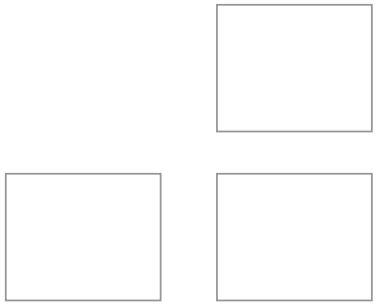
Best Data Products Inc.
DSL502E_EU

User's Manual
Revision 1.0



Copyright

This manual may not be copied, photocopied, transmitted, or translated into language or computer language, in any form, or by any means, in whole or in part, without the prior written consent by the manufacturer.

© Copyright 2002 All rights reserved.

Disclaimer

The manufacturer makes no representations or warranties, expressed, statutory or implied, regarding the fitness or merchantability of this product for any particular purpose. Further, the manufacturer is no liable for any damages, including but not limited to, lost profits, lost saving, or other incidental or consequential damages arising out of the use of this product. The manufacturer also reserves the right to make any improvements or modifications to the product described in this manual at any time, without notice of these changes.

Federal Communications Commission (FCC) NOTICE

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient of relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio / TV technician for help.

This unit was tested with shielded cables on the peripheral devices. Shielded cables must be used with the unit to insure compliance. This statement can be deleted if unit was not tested with shielded cables.

The manufacture is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference that may cause undesired operation.

CAUTION

Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

IMPORTANT SAFETY INSTRUCTIONS

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following;

1. Do not use this product near water, for example near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
2. Avoid using a telephone (other then a cordless type) during an electrical storm. There may be a remote risk of electric shock from lighting.
3. Do not use the telephone to report a gas leak in the vicinity of the Leak.
4. Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal Instructions.

SAVE THESE INSTRUCTIONS

Comment [CT1]: Add FCC statements, legal, copyright info, etc. Your equipment must be designed to meet all appropriate UL, IEC, FCC, and other requirements which apply to the jurisdiction where it will be used. For example, "This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules."

Table of Contents

1 INTRODUCTION 1

Features 1

System Requirements 1

2 GETTING TO KNOW THE BEST DATA DSL542 2

Parts Check 2

Front Panel 3

Rear Panel 4

3 HARDWARE CONNECTION AND PC CONFIGURATION 5

Connecting Your Best Data DSL542 5

Configuring Your Computers 6

4 GETTING STARTED WITH THE CONFIGURATION MANAGER 15

Accessing the Configuration Manager 15

Functional Layout 16

Changing Your Login Password 17

Committing Your Changes and Rebooting the Device 17

5 SETTING THE LAN IP ADDRESS 19

Ethernet, USB, or Both? 19

Configuring the LAN IP Address 19

Configuring the USB Port IP Address 21

6 CONFIGURING DYNAMIC HOST CONFIGURATION PROTOCOL 23

Configuring DHCP Server 23

Configuring DHCP Relay 27

Setting the DHCP Mode 28

7 CONFIGURING NETWORK ADDRESS TRANSLATION 29

Your Default NAT Setup 29

Viewing NAT Global Settings and Statistics 29

Viewing NAT Rules and Rule Statistics 31

Viewing Current NAT Translations 32

Adding NAT Rules 33

8 CONFIGURING IP ROUTES 41

Viewing the IP Routing Table 41

Adding IP Routes 42

9 CONFIGURING THE ATM VCC 44

Viewing Your ATM VC Setup 44

Adding ATM VCCs 45

Modifying ATM VCCs 46

10 CONFIGURING PPP INTERFACES 47

Viewing Your Current PPP Configuration 47

Viewing PPP Interface Details 49

Adding a PPP Interface Definition 51

Modifying and Deleting PPP Interfaces 52

11 CONFIGURING EOA INTERFACES 53

Viewing Your EOA Setup 53

Adding EOA Interfaces 54

12 CONFIGURING IPOA INTERFACES 56

Viewing Your IPoA Interface Setup 56

Adding IPoA Interfaces 57

13 CONFIGURING BRIDGING 59

Using the Bridging Feature 59

Defining Bridge Interfaces 59

Deleting a Bridge Interface 60

A TROUBLESHOOTING 61

Diagnosing Problem using IP Utilities 63

1 Introduction

Congratulations on becoming the owner of the Best Data DSL542 ADSL Ethernet bridge/router. Your LAN (local area network) will now be able to access the Internet using your high-speed ADSL connection.

This User Guide will show you how to install and set up the Best Data DSL542 ADSL Bridge/Router, and how to customize its configuration to get the most out of your new product.

Features

- Internal ADSL modem for high-speed Internet access
- 10/100Base-T Ethernet router to provide Internet connectivity to all computers on your LAN
- USB port for connecting a USB-enabled PC (Option)
- Network address translation (NAT), Firewall, and IP filtering functions to provide security for your LAN
- Network configuration through DHCP Server and DHCP Relay
- Services including IP route and DNS configuration, RIP, and IP and DSL performance monitoring
- Configuration program you access via an HTML browser

System Requirements

In order to use the Best Data DSL542 ADSL/Ethernet router, you must have the following:

- ADSL service up and running on your telephone line, with at least one public Internet address for your LAN
- One or more computers each containing an Ethernet 10Base-T/100Base-T network interface card (NIC) and/or a single computer with a USB port
- An Ethernet hub/switch, if you are connecting the device to more than one computer on an Ethernet network.

  For system configuration using the supplied web-based program: a web browser such as Internet Explorer v5.0 or later, or Netscape v4.7 or later

2 Getting to Know the Best Data DSL542

Parts Check

In addition to this document, your Best Data DSL542 should arrive with the following:

- One Best Data DSL542 ADSL Ethernet Bridge/Router
- One Power adapter and power cord
- One USB cable (Option)
- One Ethernet cable ("straight-through" type)
- One RJ-11 telephone cord
- One CD-ROM (This manual and/or USB Driver)

Front Panel

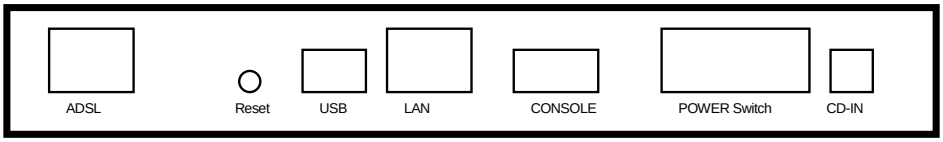
The front panel contains lights called LEDs that indicate the status of the unit.

Figure 1. Front Panel and LEDs

LED		Status	Description
POWER		Glowing	Power on
		Dim	Power off
WAN	LINK	Glowing	The WAN port is successfully linked with ADSL line
		Dim	The WAN port is not linked with any ADSL line
	DATA	Glowing	The WAN port is receiving/transmitting data
		Dim	The WAN port is not receiving/transmitting data
LAN	10	Glowing	The LAN port is connected to a 100M Ethernet device
		Flashing	The LAN port is receiving/transmitting data
	100	Glowing	The LAN port is connected to a 10M Ethernet device
		Dim	The LAN port is receiving/transmitting data

Rear Panel

The rear panel contains the ports for the unit's data and power connections.



Comment [CT2]: Insert photo of front-panel LED. Also, change table to reflect the LEDs you implemented and their labels.

Figure 2. Rear Panel Connections

ADSL	Connects the device to the wall jack for Internet connection
RESET	Resets the device to default configuration values.
USB (Option)	Connects to the USB port on your PC.
LAN	Connects the device to your PC's Ethernet port, or to the uplink port on your LAN's hub, using the cable provided.
CONSOLE (Option)	Using a special cable to connect to your computer for configuration
DC IN	Connects to the supplied power converter cable.

Comment [CT3]: True?

3 Hardware Connection and PC configuration

Connecting Your Best Data DSL542

In this part, you connect the device to the phone jack, the power outlet, and your computer or network.

Figure 4 illustrates the hardware connections. Refer to the steps that follow for specific instructions.

WARNING

Before you begin, turn the power off for all devices. *These include your computer(s), your LAN hub/switch (if applicable), and the Best Data DSL542.*

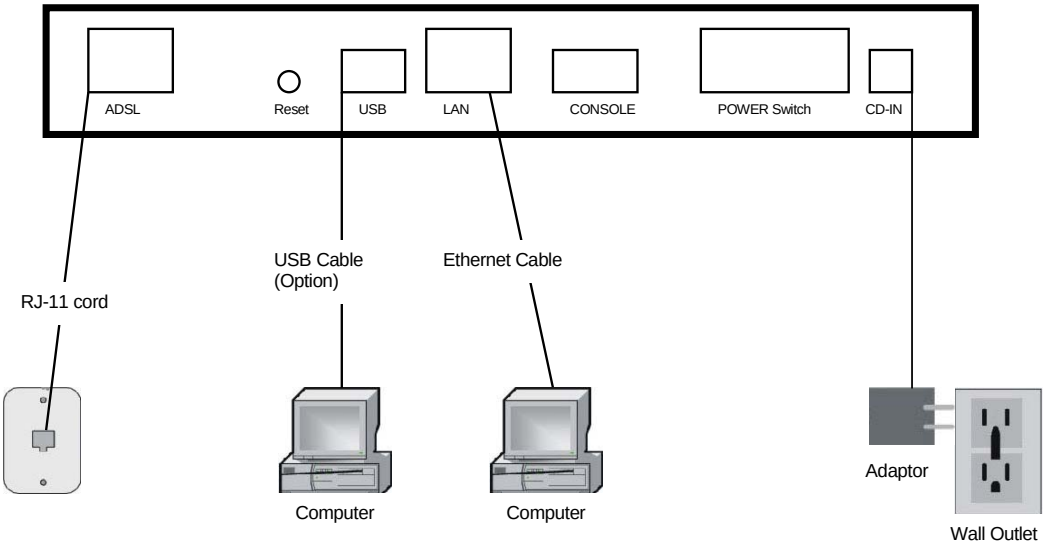


Figure 3. Overview of Hardware Connections

Step 1. Connect the ADSL cable

Connect one end of the provided phone cable to the port labeled ADSL on the rear panel of the device. Connect the other end to your wall phone jack.

Step 2. Connect the Ethernet cable.

If you are connecting a LAN to the Best Data DSL542 ADSL/Ethernet router, attach one end of a provided Ethernet cable to a regular hub port and the other to the Ethernet port on the Best Data DSL542.

If you are using the Best Data DSL542 with a single computer and no hub, you must use a "crossover" Ethernet cable (not provided) to attach the PC directly to the device. The crossover cable is wired differently than the cable you would use to connect to a hub. When you compare the colored wires on each end of a straight-through cable, they will be in the same sequence; on crossover cables, they will not. Contact your ISP for assistance.

Step 3. Attach the power connector.

Connect the AC power adapter to the PWR connector labeled DC IN on the back of the device and plug in the adapter to a wall outlet or power strip.

Step 4. Power up your systems.

Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

Step 5: Install USB software and connect the USB cable. (USB port is ontional)

You can attach a single computer to the device using a USB cable. The USB port is useful if you have an USB-enabled PC that does not have a network interface card for attaching to your Ethernet network.

Before attaching the USB cable, you must install a USB driver and configure the computer. For complete instructions, see page 10.

Configuring Your Computers

This part provides instructions for configuring the Internet settings on your computers to work with the Best Data DSL542.

Before you begin

By default, the Best Data DSL542 automatically assigns all required Internet settings to your PCs. You need only to configure the PCs to accept the information when it is assigned.

Note

*In some cases, you may want to assign Internet information manually to some or all of your computers rather than allow the Best Data DSL542 to do so. See "**Assigning static Internet information to your PCs**" on page 9 for instructions.*

- If you have connected your PC via the USB port, see the USB configuration instructions on page 10.
- If you have connected your PC of LAN via Ethernet to the Best Data DSL542, follow the instructions that correspond to the operating system installed on your PC.

Windows® 95, 98 PCs:

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
2. Double-click the Network icon.

   The Network dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled. Skip to step 9.
3. If TCP/IP does not display as an installed component, click Add....

   The Select Network Component Type dialog box displays.
4. Select **Protocol**, and then click Add....

   The Select Network Protocol dialog box displays.
5. Click on **Microsoft** in the Manufacturers list box, and then click **TCP/IP** in the Network Protocols list box.
6. Click OK to return to the Network dialog box, and then click OK again.

   You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
7. Click OK to restart the PC and complete the TCP/IP installation.

   Next, configure the PCs to accept IP information assigned by the Best Data DSL542:
8. Open the Control Panel window, and then click the Network icon.
9. Select the network component labeled TCP/IP, and then click Properties.

   If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
10. In the TCP/IP Properties dialog box, click the IP Address tab.
11. Click the radio button labeled **Obtain an IP address automatically**.
12. Click the DNS Configuration tab, and then click the radio button labeled **Obtain an IP address automatically**.
13. Click OK twice to confirm and save your changes.

    You will be prompted to restart Windows.
14. Click Yes.

Windows NT 4.0 workstations:

First, check for the IP protocol and, if necessary, install it:

1. In the Windows NT task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
2. In the Control Panel window, double click the Network icon.
3. In the Network dialog box, click the Protocols tab.

The Protocols tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to step 9.

4. If TCP/IP does not display as an installed component, click Add....
5. In the Select Network Protocol dialog box, select **TCP/IP**, and then click OK.

   You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.

   After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.

6. Click Yes to continue, and then click OK if prompted to restart your computer.

Next, configure the PCs to accept IP information assigned by the Best Data DSL542:

7. Open the Control Panel window, and then double-click the Network icon.
8. In the Network dialog box, click the Protocols tab.
9. In the Protocols tab, select **TCP/IP**, and then click Properties.
10. In the Microsoft TCP/IP Properties dialog box, click the radio button labeled **Obtain an IP address from a DHCP server**.
11. Click OK twice to confirm and save your changes, and then close the Control Panel.

Windows 2000 PCs:

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
2. Double-click the Network and Dial-up Connections icon.
3. In the Network and Dial-up Connections window, right-click the Local Area Connection icon, and then select **Properties**.

   The Local Area Connection Properties dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.

4. If Internet Protocol (TCP/IP) does not display as an installed component, click Install....
5. In the Select Network Component Type dialog box, select **Protocol**, and then click Add....
6. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click OK.

   You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.

7. If prompted, click OK to restart your computer with the new settings.

Next, configure the PCs to accept IP information assigned by the Best Data DSL542:

8. In the Control Panel, double-click the Network and Dial-up Connections icon.

9. In Network and Dial-up Connections window, right-click the Local Area Connection icon, and then select **Properties**.
10. In the Local Area Connection Properties dialog box, select **Internet Protocol (TCP/IP)**, and then click

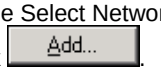
.
11. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Obtain an IP address automatically**. Also click the radio button labeled **Obtain DNS server address automatically**.
12. Click

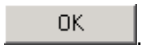
twice to confirm and save your changes, and then close the Control Panel.

Windows Me PCs

1. In the Windows task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
2. Double-click the Network and Dial-up Connections icon.
3. In the Network and Dial-up Connections window, right-click the Network icon, and then select **Properties**.

   The Network Properties dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 11.
4. If Internet Protocol (TCP/IP) does not display as an installed component, click

.
5. In the Select Network Component Type dialog box, select **Protocol**, and then click 

.
6. Select **Microsoft** in the Manufacturers box.
7. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click 

.

   You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.
8. If prompted, click

to restart your computer with the new settings.

   Next, configure the PCs to accept IP information assigned by the Best Data DSL542:
9. In the Control Panel, double-click the Network and Dial-up Connections icon.
10. In Network and Dial-up Connections window, right-click the Network icon, and then select **Properties**.
11. In the Network Properties dialog box, select **TCP/IP**, and then click

.
12. In the TCP/IP Settings dialog box, click the radio button labeled **Server assigned IP address**. Also click the radio button labeled **Server assigned name server address**.
13. Click

twice to confirm and save your changes, and then close the Control Panel.

Assigning static Internet information to your PCs

- In some cases, you may want to assign Internet information to some or all of your PCs directly (often called "statically"), rather than allowing the Best Data DSL542 to assign it.

Before you begin, contact your ISP if you do not already have the following information:

- The IP address and subnet mask to be assigned to each PC to which you will be assigning static IP information.
- The IP address of the default gateway for your LAN. In most cases, this is the address assigned to the LAN port on the Best Data DSL542. By default, the LAN port is assigned this IP address: **192.168.1.1**. (You can change this number, or another number can be assigned by your ISP. See Chapter 5 for more information.)
- The IP address of your ISP's Domain Name System (DNS) server.

On each PC to which you want to assign static information, follow the instructions on pages 7 through 9 relating only to checking for and/or installing the IP protocol. Once it is installed, continue to follow the instructions for displaying each of the Internet Protocol (TCP/IP) properties. Instead of enabling dynamic assignment of the IP addresses for the computer, DNS server, and default gateway; click the radio buttons that enable you to enter the information manually.

Note

Your PCs must have IP addresses that place them in the same subnet as the Best Data DSL542's LAN port. If you manually assign IP information to all your LAN PCs, you can follow the instructions in Chapter 5 to change the LAN port IP address accordingly.

Configuring a computer connected to the USB port

If the Best Data DSL542 includes a USB port for connecting to a PC, you must install the provided USB driver software on the PC. The driver enables Ethernet-over-USB communication with the Best Data DSL542.

Configuring the USB computer is a two-part process:

- In Part 1, you install the USB driver on the PC.
- In Part 2, you configure the IP properties on the USB PC.

Before you start to install USB driver, you shall create an entry for USB port via RS-232 serial cable.

1. Connect an RS-232 cable from one serial COM port on your PC to the Best Data DSL542
2. In Windows, go to **Start** → **Programs** →**Accessories** → **Communications** → **HyperTerminal**
3. When the HyperTerminal window appears, double-click **Hypertrm** to start a new session.
4. Name the new connection and select an icon for this session
5. In the **Connect To** dialog box, select the COM port that you used to connect to this product.
6. In the COM port Properties dialog box, set the serial port setting at 38400 baud rate, 8 bit, none parity, none flow control.
7. Type "**create usb intf ifname usb-0 ip 198.168.1.2 mask 255.255.255.0 inside**" then Enter
8. You will see "Entry created" then you have to type "commit" to save this entry.

Part 1. Installing the USB Driver:

1. Ensure that the USB cable **is not connected** to the USB port on the PC or to the USB port on the Best Data DSL542. The installation program will prompt you when to connect the cable.
2. Copy the USB installation file to a temporary directory on the USB computer.
3. In the folder where you copied the files, double-click on *setup.exe* to start the installation program. The Welcome dialog box displays, as shown in Figure :

Welcome
Welcome to the GlobeSpan DSL Modem Setup program. This program will install the GlobeSpan DSL Modem on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
InstallShield
Next >
Cancel

Figure 4. USB Driver Installation: Welcome Screen

4. Click to display the Software License Agreement dialog box, as shown in Figure .

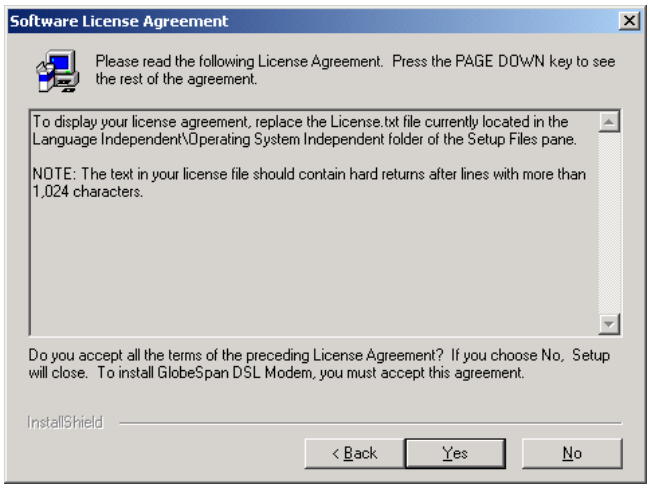
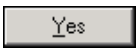
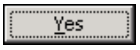

Software License Agreement
Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.
To display your license agreement, replace the License.txt file currently located in the Language Independent\Operating System Independent folder of the Setup Files pane.
NOTE: The text in your license file should contain hard returns after lines with more than 1,024 characters.
Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install GlobeSpan DSL Modem, you must accept this agreement.
InstallShield
< Back
Yes
No

Figure 5. USB Driver Installation: Software License Agreement

5. After reviewing the license agreement, click  to continue.
6. If a Microsoft digital signature dialog box displays, click  to continue.

The installation program will begin copying the necessary installation files to the required locations. When finished, the Setup Complete dialog box will display, as shown in Figure .

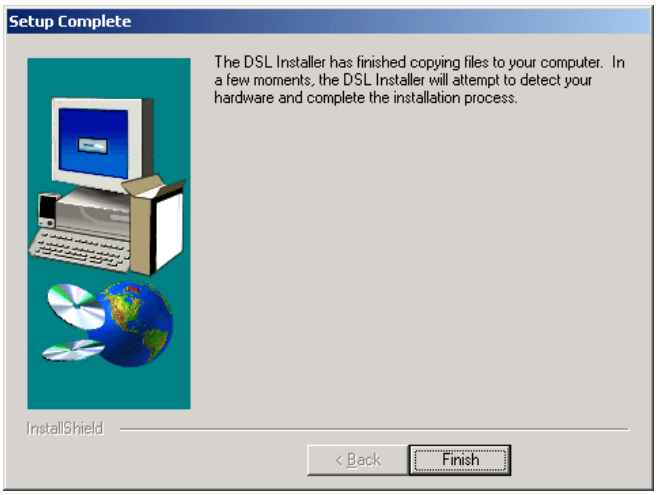

Setup Complete
The DSL Installer has finished copying files to your computer. In a few moments, the DSL Installer will attempt to detect your hardware and complete the installation process.
InstallShield
< Back
Finish

Figure 6. USB Driver Installation: Setup Complete

7. Click Finish.

A DSL Installer dialog box displays while the program searches for your USB hardware. After a few seconds, a second dialog box displays to prompt you to attach the USB cable, as shown in Figure .

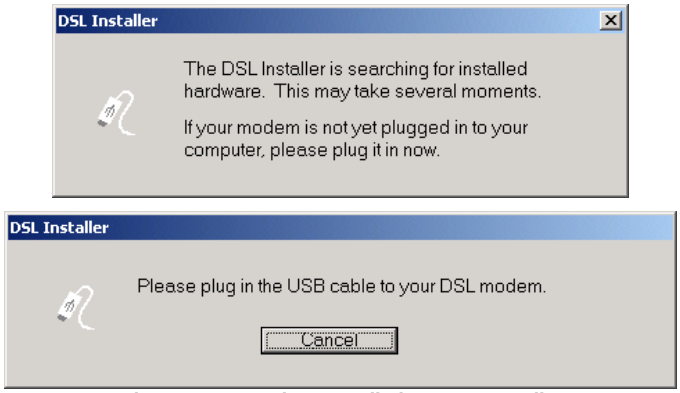

DSL Installer
The DSL Installer is searching for installed hardware. This may take several moments.
If your modem is not yet plugged in to your computer, please plug it in now.
DSL Installer
Please plug in the USB cable to your DSL modem.
Cancel

Figure 7. USB Driver Installation: DSL Installer

8. Attach the USB cable to the Best Data DSL542 and to your PC.

The USB cable provided has a flat connector on one end (called Type A) and a square connector on the other (Type B). Connect the flat connector to your PC and the square connector to the Best Data DSL542.

A window displays briefly, indicating that the system has found new hardware.

9. If a Microsoft digital signature dialog box displays, click Yes to continue.

The System Settings Change dialog box displays to prompt you to restart your computer, as shown in Figure :

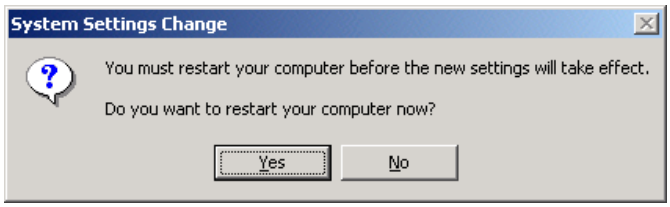
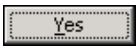

System Settings Change
You must restart your computer before the new settings will take effect.
Do you want to restart your computer now?
Yes
No

Figure 8. USB Driver Installation: System Settings Change

9. Click  to restart your computer.

When your computer finishes rebooting, make sure that the GlobeSpan installer program displays as an item on your Windows Start menu:

10. Click the Start button, point to **Programs » GlobeSpan DSL Modem**, and click on **Configure**.

    The DSL Modem Installer dialog box should display, as shown in Figure .

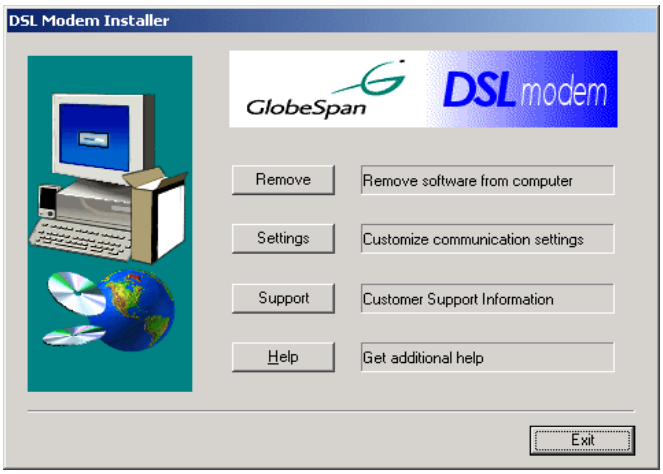


Figure 9. DSL Modem Installer Dialog Box

This step is only verification. You do not need to access the configuration program at this time.

11. Click .

Part 2. Configuring IP properties on the USB PC.

Now that the USB driver installation is complete, you must configure the USB PC so that its IP properties place it on the same subnet as the Best Data DSL542's USB port. There are two ways to do this:

- The Best Data DSL542 is configured to assign an appropriate IP address to the USB PC. If you want to use this automatic assignment feature, called "DHCP server," you must configure the USB PC to accept dynamically assigned IP information. Follow the instruction on pages 7 through 9 that correspond to the operating system installed on the PC.
- If you want to assign a static IP address to the PC, follow the instructions on page 9 and use the following information.
  - In the Network and Dial-up Connections window, be sure to select the icon that corresponds to your new USB connection (not the one that corresponds to your

Ethernet NIC). When you display the properties for the icon, the following text should display in the Connect Using text box:

GlobeSpan USB IAD LAN Modem #n

- The USB port on the Best Data DSL542 is preconfigured with these properties (you cannot change these values):

  USB port IP address: 198.168.1.2
  USB port subnet mask: 255.255.255.0

  Therefore, your PC must be configured as follows:

  IP address: 192.168.2.*n* where *n* is a number from *2* to *254*.

  Subnet mask: 255.255.255.0

  Default gateway: *198.168.1.2*

Default Router Settings

In addition to handling the DSL connection to your ISP, the Best Data DSL542 ADSL/Ethernet router can provide a variety of services to your network. The device is preconfigured with default settings for use with a typical home or small office network.

Table 1 lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration, review the settings in Table 1 to verify that they meet the needs of your network. Follow the instructions to change them if necessary. If you are unfamiliar with these settings, try using the device without modification, or contact your ISP for assistance.

Before you modifying any settings, review Chapter 4 for general information about accessing and using the Configuration Manager program. We strongly recommend that you contact your ISP prior to changing the default configuration.

Table 1. Default Settings Summary

Option	Default Setting	Explanation/Instructions
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with two pools of addresses: For LAN computers: 192.168.1.3 through 192.168.1.34 For USB computer: 192.168.1.2 (for both, subnet mask = 255.255.255.0)	The Best Data DSL542 maintains a pool of 32 private IP addresses for dynamic assignment to your LAN computers and a pool containing 1 IP address for assignment to your USB computer. To use this service, you must have set up your computers to accept IP information dynamically. See Chapter 6 for an explanation of the DHCP service.
NAT (Network Address Translation)	napt rule enabled	Your computers' private IP addresses (see DHCP above) will be translated to your public IP address whenever they access the Internet. See Chapter 7 for a description of the NAT service.
LAN Port IP Address	Static IP address: 192.168.1.1 subnet mask: 255.255.255.0	This is the IP address of the LAN port on the device. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See Chapter 5 for instructions.
USB Port IP Address	Assigned static IP address: 198.168.1.2 subnet mask: 255.255.255.0	This is the IP address assigned to the USB port on the device (if used). Typically, you will not need to change this address. See Chapter 5 for instructions.

4 Getting Started with the Configuration Manager

The Best Data DSL542 includes preinstalled program called the *Configuration Manager*, which provides an interface to the software installed on the device. It enables you to configure the device settings to meet the needs of your network. You access it through your web browser from any PC connected to the Best Data DSL542 via the LAN port.

Note

The Best Data DSL542 may already be configured to provide Internet connectivity for your network. If it works properly with the preconfigured settings, then you may not need to use the Configuration Manager. Contact your ISP to determine which settings you may need to change, if any.

Accessing the Configuration Manager

The Configuration Manager program is preinstalled into memory on the Best Data DSL542. To access the program, you need the following:

- A PC or laptop connected to the LAN port on the Best Data DSL542.
- A web browser installed on the PC. The program is designed to work best with Microsoft Internet Explorer® version 5.0, Netscape Navigator® version 4.7, or later versions.

You can access the program from any computer connected to the Best Data DSL542 via the LAN or USB ports.

1. From a LAN computer, open your web browser, type the following URL in the web address (or location) box, and press **<Enter>**:

`http://192.168.1.1`

Or, from the USB computer, type:

`http://198.168.1.2`

These are the predefined IP addresses for the LAN and USB ports on the Best Data DSL542.

A login screen displays, as shown in Figure .

Figure 10. Login Screen

2. Enter your user name and password, and then click OK.
3. The first time you log into the program, use these defaults:

Default User Name: root
Default Password: root

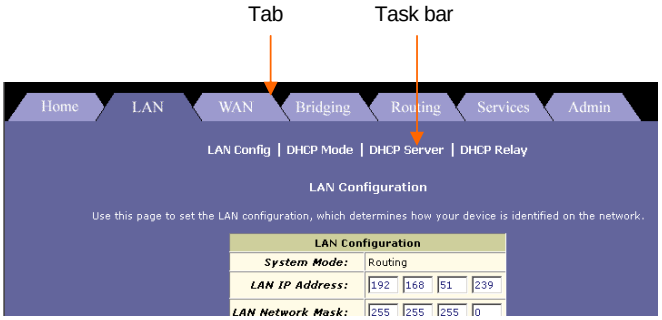
Comment [CT4]: Replace with the default user ID and password that you preconfigure on your product, if different. Search for and replace throughout.

Note

You can change the password at any time (see Changing Your Login Password on page 17). The user name cannot be changed.

Functional Layout

Configuration Manager tasks are grouped into categories, which you can access by clicking the tabs at the top of each page. You can click on these to display the specific configuration options.



A separate page displays for each task in the task bar. The left-most task displays by default when you click on a new tab. The same task may appear in more than one tab, when appropriate. For example, the Lan Config task displays in both the LAN tab and the Routing tab.

Commonly used buttons

The following buttons are used throughout the application.

Button	*Function*
Submit	Stores in *temporary* system memory any changes you have made on the current page. See "**Committing your changes**" on page 17 for instructions on storing changes permanently.
Refresh	Redisplays the current page with updated statistics.
Clear	When accumulated statistics are displaying, this button resets the statistics to their initial values.
Help	Launches the online help for the current topic in a separate browser window. Help is available from any main topic page.

Changing Your Login Password

The first time you log into the Configuration Manager, you use the default user ID and password (*root* and *root*). The system allows only one user ID and password. Only the password can be changed.

Note

This user ID and password is only used for logging into the Configuration Manager; it is not the same as the login you may use to connect to your ISP (described in Chapter 11).

To change the Configuration Manager login password:

1. Click the Admin tab.

The User Password Configuration page displays by default.

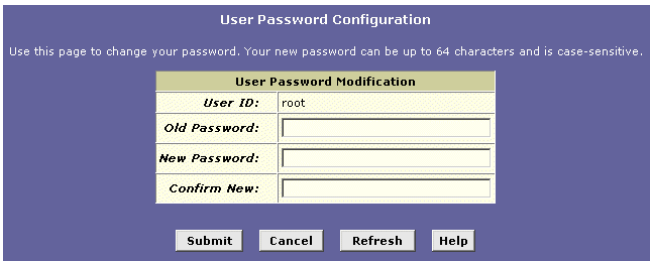


Figure 11. User Password Configuration Page

2. Type your current password in the Old Password text box.
3. Type the new password in the New Password text box and again in the Confirm New text box.

The password can be up to eight ASCII characters long. When logging in, you must type the new password in the same upper and lower case characters that you use here.

4. Click Submit.
5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
6. Click Commit to save your changes to permanent memory.

Committing Your Changes and Rebooting the Device

Committing your changes

Whenever you use the Configuration Manager to change system settings, the changes are initially placed in temporary storage. Your changes are made effective when you submit them, but will be lost if the device is reset or turned off.

To save your changes for future use, you can use the commit function.

Note

***Submitting** changes saves them only until the device is reset or powered down. **Committing** changes saves them permanently.*

Follow these steps to commit changes to permanent storage.

1. Click the Admin tab, and then click **Commit & Reboot** in the task bar.

The Commit & Reboot page displays:

Figure 12. Commit & Reboot Page

2. Click Commit. (Disregard the selection in the Reboot Mode drop-down list; it does not affect the commit process.)

The changes are saved to permanent storage.

The previous settings are copied to backup storage so that they can be recalled if your new settings do not work properly (see the rebooting instructions on page 18).

Rebooting the device using Configuration Manager

To reboot the device, display the Commit and Reboot page, select the appropriate reboot mode from the drop-down menu, and then click Reboot.

You can select from the following three options when rebooting:

Option	Description
Reboot from Last Configuration	Reboots the device using the current settings in permanent memory, including any changes you just committed.
Reboot from Backup Configuration	Reboots the device using settings stored in backup memory. These are the settings that were in effect before you committed new settings in the current session.
Reboot from Default Configuration	Reboots the device to default settings provided by your ISP or the manufacturer. Choosing this option erases any custom settings.

WARNING

Do not reboot the device using the Reset button on the back panel of the Best Data DSL542 to activate new changes. This button resets the device settings to the manufacturer's default values. Any custom settings will be lost.

5 Setting the LAN IP Address

This chapter describes how to configure the interfaces on the ADSL/Ethernet router that communicate with your LAN and USB computers.

Ethernet, USB, or Both?

If you are using the ADSL/Ethernet router with multiple PCs on your LAN, you must connect the LAN via an Ethernet hub to the device's LAN port, called eth-0.

If you are using a single PC with the ADSL/Ethernet router, you have two options for connecting it to the device:

- You can connect the PC directly to the LAN port using a crossover Ethernet cable. See Appendix A, "Troubleshooting" for a description of crossover versus straight-through Ethernet cables.
- If the PC is USB-enabled, you can connect it directly to the device's USB port, called usb-0. Only one computer can be connected in this manner.

You can also use the USB and Ethernet ports simultaneously, connecting your LAN to the Ethernet port and a standalone PC to the USB port. (USB port is an option)

You must assign a unique IP address to each device port that you use.

Note

The instructions that follow assume that the device has been preconfigured to operate in Routing mode, which uses the IP protocol to determine how to exchange data among your PCs, the device, and your ISP. If your device is configured in Bridging mode, its ports do not require IP addresses. The operating mode displays at the top of the LAN Configuration page and cannot be changed by the user.

Configuring the LAN IP Address

The LAN IP address identifies the LAN port (eth-0) as a node on your network; that is, its IP address must be in the same subnet as the PCs on your LAN.

Definition

*A **network node** can be thought of as any interface where a device connects to the network, such as the Best Data DSL542's LAN port and the network interface cards on your PCs.*

You can change the default to reflect the set of IP addresses that you want to use with your network.

If your network uses a local DHCP server (other than the ADSL/Ethernet router) to assign IP addresses, you can configure the device to accept and use a LAN IP address assigned by that server. In this mode, the ADSL/Ethernet router is considered a *DHCP client* of your DHCP server.

Note

*The Best Data DSL542 itself can function as a DHCP server for your LAN computers, as described in Chapter 5, **but not for its own LAN port**.*

Follow these steps to change the default LAN IP address or to configure the LAN port as a DHCP client.

1. Log into Configuration Manager, and then click the LAN tab.

   The LAN Configuration page displays, as shown in Figure .

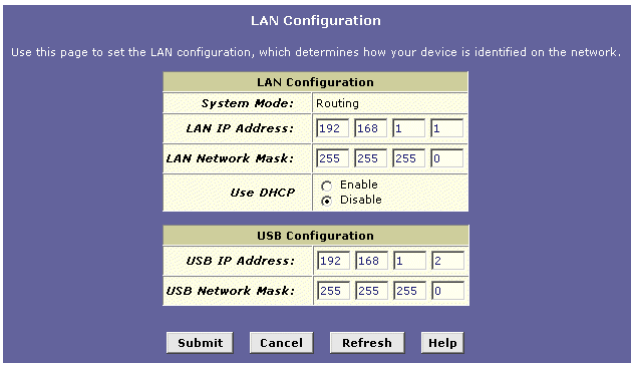


Figure 13. LAN Configuration Page

The LAN Configuration table displays the following settings:

Setting	Description
System Mode	The preconfigured mode for your device, such as Routing or Bridging mode. This setting is not user - configurable.
LAN IP Address	The IP address your computers use to identify the device's LAN port. Note that the public IP address assigned to you by your ISP **is not** your LAN IP address. The public IP address identifies the WAN (ADSL) port on your ADSL/Ethernet router to the Internet.
LAN Network Mask	The LAN Network mask identifies which parts of the LAN IP Address refer to your network as a whole and which parts refer specifically to nodes on the network. Your device is preconfigured with a default network mask of 255.255.255.0.
Use DHCP	When checked, this setting instructs the device to accept LAN IP information assigned dynamically from another DHCP server already configured on your network. The Best Data DSL542 cannot act as a DHCP server for its own LAN port.

2. Enter a LAN IP address and network mask, or click the DHCP **Enable** radio button.

   - **Entering a fixed address:** If you are using routing services on you LAN such as DHCP and NAT, you will want to assign a fixed LAN IP address and mask. This ensures that your LAN computers have a fixed address that they use to communicate with the device.

     The IP address you assign must be on the same subnet as your LAN computers that connect to this port (that is, the network ID portion of their IP addresses and their subnet masks must be the same).

You may need to update the DHCP configuration so that the addresses that the DHCP server dynamically assigns to your computers are on the same subnet as the new LAN IP address. See Chapter 6 for instructions on changing the pool of dynamically assigned addresses. In addition, if you change the DHCP pool, you will also need to update the NAT configuration so the new IP addresses are translated properly. See Chapter 7 for instructions on NAT.

- **Enabling DHCP:** If another computer on your LAN provides DHCP services for your network, you can click the Use DHCP checkbox to enable the LAN port to accept a dynamically assigned address from the server. Check with your ISP to determine if this is advisable.

  When you click the Enable radio button, the LAN Network Mask field will be dimmed (made unavailable for entry). The LAN IP Address field will remain editable, however. The address that you specify here will be used as a requested IP address from the DHCP server. This is referred to as a "Configured IP Address" in the program. If the configured IP address is not available from the DHCP server, the server will distribute another address to the LAN port. Even if another number is assigned, the same configured IP address will continue to display in this field.

  For a description of how DHCP works, see Chapter 6.

3. Click Submit.
   - If you were using an Ethernet connection for the current session, and changed the IP address, the connection will be terminated.
   - If you are currently using the USB interface, a page will display to confirm your change and your connection will remain active.
   - If you enabled the DHCP service, the ADSL/Ethernet router will initiate a request for an IP address from your LAN's DHCP server. Assuming a different IP address is assigned, your current connection will be terminated.

4. Reconfigure your PCs, if necessary, so that their IP addresses place them in the same subnet as the new IP address of the LAN port.
5. Log into Configuration Manager by typing the new IP address in your Web browser's address/location box.

   If you enabled DHCP, you may need to check the DHCP server on your LAN to determine the IP address actually assigned to the LAN port.
6. If the new settings work properly click the Admin tab, and then click **Commit & Reboot** in the task bar.
7. Click Commit to save your changes to permanent memory.

Configuring the USB Port IP Address

1. If the LAN Configuration page is not already displaying, click the LAN tab.
2. In the USB Configuration table, enter the IP Address and Network Mask for the USB port.

The IP address must place the USB port in the same subnet as the USB computer; If you are using both the LAN port and the USB port, however, the USB port and USB computer must not be in the same subnet as the LAN port or the computers attached to it.

For example, you could assign the following IP addresses to the LAN and USB ports (both assume a network mask of 255.255.255.0):

	Port IP Address	Computer(s) IP Address(es)
LAN	192.168.1.1	192.168.1.x (x = 3-254)
USB	192.168.1.2	192.168.1.x

3. Click Submit.
   - If you are currently communicating with the device via the USB interface, then the connection will be terminated, because the IP address that the connection was using has now changed.
   - If you are currently using the Ethernet interface, a page will display to confirm your change and your connection will remain active.
4. If necessary, reconfigure your USB PC so that its IP address places it in the same subnet as the new IP address of the USB port.
5. Log into Configuration Manager by typing the new USB port IP address in your Web browser's address/location box.
6. If the new settings work properly click the Admin tab, and then click **Commit & Reboot** in the task bar.
7. Click Commit to save your changes to permanent memory.

6 Configuring Dynamic Host Configuration Protocol

You can configure your network and Best Data DSL542 to use the Dynamic Host Configuration Protocol (DHCP). This chapter provides DHCP instructions for implementing it on your network.

The device can be configured as a DHCP server, DHCP relay agent, or, in some cases, a DHCP client.

Note

You can input settings for both DHCP server and DHCP relay mode, and then activate either mode at any time. De-activated settings are retained for your future use.

Configuring DHCP Server

Note

*By default, the device is configured as a DHCP server, with a predefined IP address pool of 192.168.1.2 through 192.168.1.13 (subnet mask 255.255.255.0). To change this range of addresses, see "**Viewing, modifying, and deleting address pools**" on page 25.*

First, you must configure your PCs to accept DHCP information assigned by a DHCP server:

1. Open the Windows Control Panel and display the computer's Networking properties. Configure the TCP/IP properties to "Obtain an IP address automatically" (the actual text may vary depending on your operating system).

   Next, you define the pools of IP addresses you want to make available for distribution to your computers. These addresses can be multiple public addresses that you have purchased from your ISP, but are typically private addresses that you create. (LAN administrators often create private IP addresses for use only on their networks.

2. Log into Configuration Manager, click the LAN tab, and then click **DHCP Server** in the task bar.

   The DHCP Server Configuration page displays, as shown in Figure 15.

Figure 14. DHCP Configuration Page

Each pool you create displays in a row on the table on this page.

You can create up to eight pools; however, most users will need to create only one for their LAN. Some users many want to create another that distributes an IP address to their USB computer, which must be in a different subnet than the LAN computers.

3. To add an IP address pool, click Add.

The DHCP Server Pool – Add page displays, as shown in Figure 16.

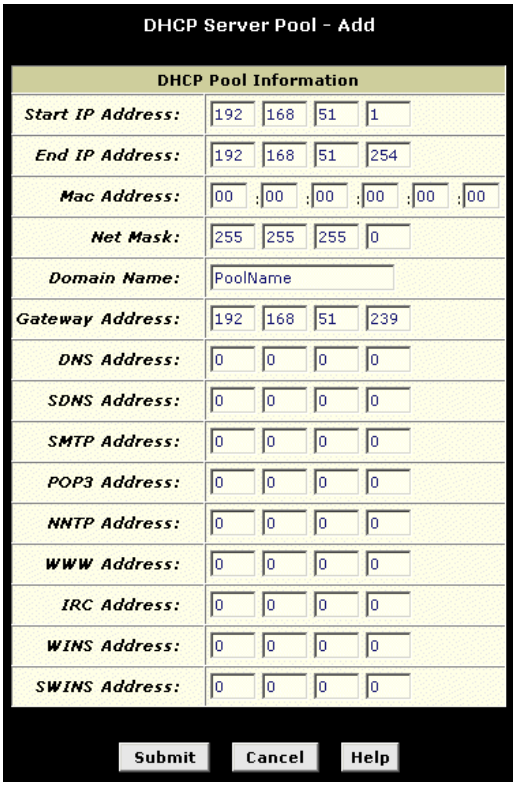

DHCP Server Pool - Add
DHCP Pool Information
Start IP Address: 192 168 51 1
End IP Address: 192 168 51 254
Mac Address: 00 :00 :00 :00 :00 :00
Net Mask: 255 255 255 0
Domain Name: PoolName
Gateway Address: 192 168 51 239
DNS Address: 0 0 0 0
SDNS Address: 0 0 0 0
SMTP Address: 0 0 0 0
POP3 Address: 0 0 0 0
NNTP Address: 0 0 0 0
WWW Address: 0 0 0 0
IRC Address: 0 0 0 0
WINS Address: 0 0 0 0
SWINS Address: 0 0 0 0
Submit
Cancel
Help

Figure 15. DHCP Server Pool – Add Page

4. Enter the *Start IP Address*, *End IP Address*, *Net Mask*, and *Gateway Address* fields are required; the others are optional. The following table describes each field.

Field	Description
Start/End IP Addresses	Specify the lowest and highest addresses in the pool.
Mac Address	Use this field only if you want to assign a specific IP address to a specific computer (that is, you are creating an exception to the dynamic assignment of addresses). The IP address you specify will be assigned to the computer that corresponds to this MAC address. (A MAC address is a manufacturer-assigned hardware ID that is unique for each device on a network.) If you type a MAC address here, you must have specified the same IP address in both the Start IP Address and End IP Address fields.

Field	Description
Net Mask	Specifies which portion of each IP address in this range refers to the network and which portion refers to the host (computer). You can use the network mask to distinguish which pool of addresses should be distributed to a particular subset of computers on your LAN (called a *subnet*).
Domain Name	A user-friendly name that refers to the group of computers (subnet) that will be assigned addresses from this pool.
Gateway Address	The address of the default gateway for computers that receive IP addresses from this pool. The default gateway is the IP address that the computers first contact to communicate with the Internet. Typically, it is the device's LAN port IP address.
DNS/SDNS Address	The IP address of the *Domain Name System* server and *Secondary Domain Name System* server to be used by computers that receive IP addresses from this pool. These DNS servers translate common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, these servers are located with your ISP.
SMTP...SWINS (optional)	The IP addresses of devices that perform various services for computers that receive IP addresses from this pool (such as the SMTP, or *Simple Mail Transfer Protocol*, server which handles e-mail traffic). Contact your ISP for these addresses.

5. Click Submit.

   A confirmation page displays briefly to indicate that the pool has been added successfully. After a few seconds, the DHCP Server Pool – Add page displays with the newly added pool.

6. Follow the instructions in "Setting the DHCP Mode" on page 28 to set the DHCP mode to DHCP Server.

Viewing, modifying, and deleting address pools, and excluding IP addresses from a pool

To view, modify, or delete an existing address pool, display the DHCP Server Configuration page, and click the icons in the corresponding row in the address pool table.

- To delete an IP address pool, click , then submit and commit your changes.
- To view details on an IP address pool, click . A page displays with all the same information you entered when adding the pool.

  To modify the domain name associated with an IP address pool, or to exclude addresses from the pool, click . The DHCP Server Pool – Modify page displays, as shown in Figure .

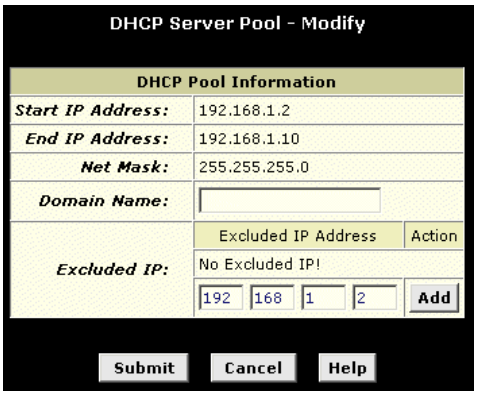


Figure 16. DHCP Server Pool – Modify Page

Excluded addresses are those that you have designated for fixed use with specific devices, or for some other reason do not want to make available to your network.

To exclude an address from distribution, type it in the fields provided and click **Add**. Click **Submit** after entering your changes. Be sure to use the Commit feature to save your changes to permanent memory, as described on page 17.

Viewing current DHCP address assignments

When the Best Data DSL542 functions as a DHCP server for your LAN, it keeps a record of any addresses it has leased to your computers. To view a table of all current IP address assignments, display the DHCP Server Configuration page, click **Address Table**.

A page displays similar to that shown in Figure :

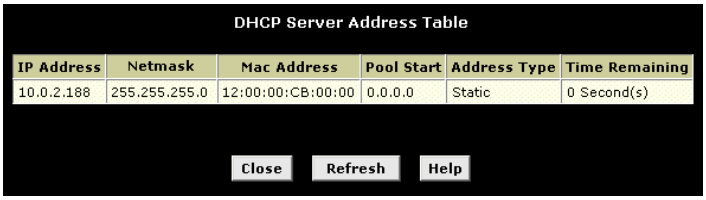


Figure 17. DHCP Server Address Table Page

The DHCP Server Address Table lists any IP addresses that are currently leased to LAN devices. For each leased address, the table lists the following information:

Field	Description
IP Address	The address that has been leased from the pool.
Netmask	The network mask associated with the leased address, which identifies the network ID and host ID portions of the address (see Appendix A).
Mac Address	A hardware ID for the device to which the number has been assigned.
Pool Start	The lower boundary of the address pool (provided to identify the pool from which the leased number came).

Field	Description
Address Type	Static or Dynamic. *Static* indicates that the IP number has been assigned permanently to the specific hardware device. *Dynamic* indicates that the number has been leased temporarily for a specified length of time.
Time Remaining	The amount of time left for the device to use the assigned address.

Configuring DHCP Relay

Some ISPs perform the DHCP server function for their customers' home/small office networks. In this case, you can configure the device as a DHCP relay agent. When a computer on your network requests Internet access, the Best Data DSL542 contacts your ISP to obtain an IP address (and other information), and then forwards that information to the computer.

First, you must configure your PCs to accept DHCP information assigned by a DHCP server:

1. Open the Windows Control Panel and display the computer's Networking properties. Configure the TCP/IP properties to "Obtain an IP address automatically" (the actual text may vary depending on your operating system).

Next, you specify the IP address of the DHCP server and select the interfaces on your network that will be using the relay service.

2. Log into the Configuration Manager, click the LAN tab, and then click **DHCP Relay** in the task bar.

The DHCP Relay Configuration page displays, as shown in Figure 19.

DHCP Relay Configuration
As a DHCP relay agent, when a computer request Internet access, the device requests an IP address from your ISP, and then relays the addresses back to the computers. This table lists each interface on the device that relays data from your ISP (typically, the LAN port is listed).
DHCP Server Address:
Interfaces Running DHCP Relay
Action
No Interface Running DHCP Relay!
eth-0
Add
Submit
Cancel
Refresh
Help

Figure 18. DHCP Relay Configuration Page

3. Type the IP address of your ISP's DHCP server in the fields provided.

If you do not have this number, it is not essential to enter it here. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.

4. If the interface named eth-0 is not already displaying, select it from the drop-down list and click **Add**.

The eth-0 interface specifies that your default Ethernet (LAN) interface is running DHCP relay for your LAN. Typically, this is the only interface you need to specify here. If the Best Data DSL542 has additional interfaces that you want to perform DHCP relay, you can select and add them.

(You can also delete an interface from the table by clicking in the right column.)

5. Click Submit.

   A page displays to confirm your changes, and then the program returns to the DHCP Relay Configuration page.

6. Follow the instructions in "Setting the DHCP Mode" on page 28 to set the DHCP mode to DHCP Relay.

Setting the DHCP Mode

You should set the DHCP mode only after you have configured DHCP relay or DHCP server settings. See "Configuring DHCP Server" on page 23 or "Configuring DHCP Relay" on page 27 for additional instructions.

Follow these instructions to set the DHCP mode:

1. Click the LAN tab, and then click **DHCP Mode** in the task bar.
2. From the DHCP Mode drop-down list, choose **DHCP Server**, **DHCP Relay**, or **none**.

   If you choose none, your LAN computers must be configured with static IP addresses.

3. Click Submit.
4. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
5. Click Commit to save your changes to permanent memory.

7 Configuring Network Address Translation

This chapter provides Network Address Translation (NAT) instructions for modifying the default configuration on your device.

Your Default NAT Setup

By default, NAT is enabled, with a napt rule configured to perform the following translation:

These private IP addresses:	...are translated to:
192.168.1.3 192.168.1.4 . . . 192.168.1.34	Your ISP-assigned public IP address

For a description of napt rules, see page 33. This default NAT setup assumes that, on each LAN computer, you configured TCP/IP properties as follows:

- You selected the check box that enables them to receive their IP addresses automatically (that is, to use a DHCP server);

  or,

- You assigned static IP addresses to your PCs in the range 192.168.1.3 through 192.168.1.34.

If your computers are not configured in one of these ways, you can either change the IP addresses on your computers to match the NAT setup or delete this NAT rule and add a new one that matches the addresses you assigned to your computers (see "Adding NAT Rules" on page 33 for instructions).

Viewing NAT Global Settings and Statistics

To view your NAT settings, log into Configuration Manager, click the Services tab. The NAT Configuration page displays by default, as shown in Figure .

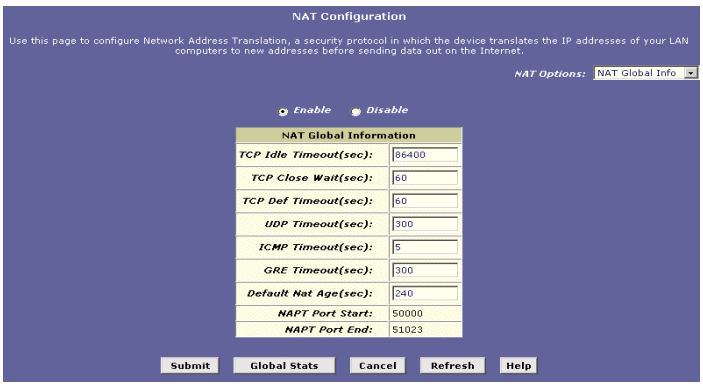


Figure 19. NAT Configuration Page

The NAT Configuration page contains the following elements:

- The NAT Options drop-down list, which provides access to the Global Information page (shown by default), the NAT Rule Configuration page, and the NAT Translations page, which shows current translations.
- Enable/Disable radio buttons, which allow you to turn on or off the NAT feature.
- The NAT Global Information table, which displays the following settings that apply to all NAT rule translations:

Field	Description
TCP Idle Timeout (sec)	For a NAT translation session on data that uses the TCP protocol, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.
TCP Close Wait (sec)	For a NAT translation on data using the TCP protocol, after a communication session has been closed, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.
TCP Def Timeout (sec)	For a NAT translation session on data that uses the TCP protocol, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.
UDP Timeout (sec)	Same as TCP Idle Timeout, but for UDP packets.
ICMP Timeout (sec)	Same as TCP Idle Timeout, but for ICMP packets.
GRE Timeout (sec)	Same as TCP Idle Timeout, but for GRE packets.
Default Nat Age (sec)	For all other NAT translation sessions, the number of seconds after which a translation session will no longer be valid.
NAPT Port Start/End	When a napt rule is defined, the source ports will be translated to sequential numbers in this range.

If you change any values, click Submit, and then click the Admin tab and commit your changes to permanent system memory (see page 17).

You can click Global Stats to view accumulated data on how many NAT rules have been invoked and how much data has been translated. A page similar to the one is shown in Figure displays.

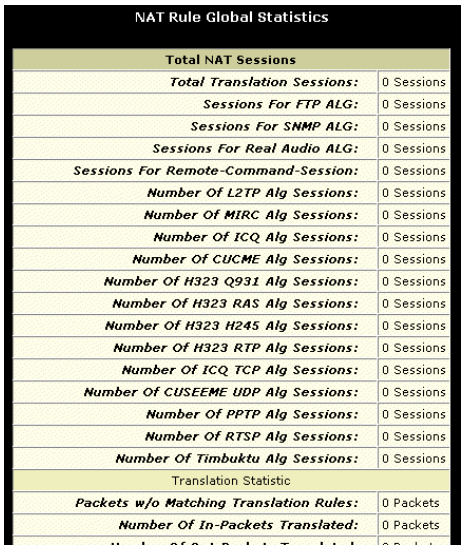

NAT Rule Global Statistics
Total NAT Sessions
Total Translation Sessions: 0 Sessions
Sessions For FTP ALG: 0 Sessions
Sessions For SNMP ALG: 0 Sessions
Sessions For Real Audio ALG: 0 Sessions
Sessions For Remote-Command-Session: 0 Sessions
Number Of L2TP Alg Sessions: 0 Sessions
Number Of MIRC Alg Sessions: 0 Sessions
Number Of ICQ Alg Sessions: 0 Sessions
Number Of CUCME Alg Sessions: 0 Sessions
Number Of H323 Q931 Alg Sessions: 0 Sessions
Number Of H323 RAS Alg Sessions: 0 Sessions
Number Of H323 H245 Alg Sessions: 0 Sessions
Number Of H323 RTP Alg Sessions: 0 Sessions
Number Of ICQ TCP Alg Sessions: 0 Sessions
Number Of CUSEEME UDP Alg Sessions: 0 Sessions
Number Of PPTP Alg Sessions: 0 Sessions
Number Of RTSP Alg Sessions: 0 Sessions
Number Of Timbuktu Alg Sessions: 0 Sessions
Translation Statistic
Packets w/o Matching Translation Rules: 0 Packets
Number Of In-Packets Translated: 0 Packets

Figure 20. NAT Rule Global Statistics Page

The table provides basic information for each NAT rule you have set up. You can click **Clear** to restart the accumulation of the statistics at their initial values.

Viewing NAT Rules and Rule Statistics

To view the NAT rules currently defined on your system, select **NAT Rule Entry** in the NAT Options drop-down list. The NAT Rule Configuration page displays, as shown in Figure .

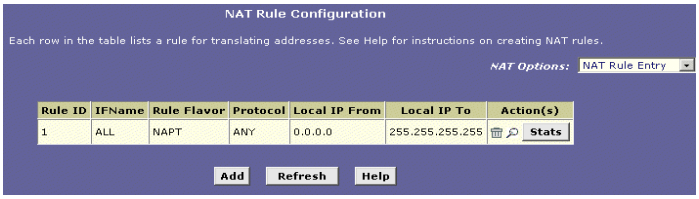


Figure 21. NAT Rule Configuration Page

The NAT Rule Configuration table displays a row containing basic information for each rule. For a description of these fields, refer to the instructions for adding rules (pages 33 through 39).

From the NAT Rule Configuration page, you can click **Add** to add a new rule, or use the icons in the right column to delete (🗑) or view details on (🔎) a rule.

To view data on how often a specific NAT rule has been used, click **Stats** in the Action(s) column. A page similar to the one show in Figure displays:

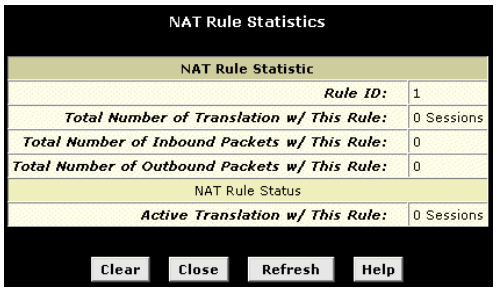

NAT Rule Statistics
NAT Rule Statistic
Rule ID: 1
Total Number of Translation w/ This Rule: 0 Sessions
Total Number of Inbound Packets w/ This Rule: 0
Total Number of Outbound Packets w/ This Rule: 0
NAT Rule Status
Active Translation w/ This Rule: 0 Sessions
Clear
Close
Refresh
Help

Figure 22. NAT Rule Statistics Page

The statistics show how many times this rule has been invoked and how many currently active sessions are using this rule. You can click Clear to reset the statistics to zeros and Refresh to display newly accumulated data.

Viewing Current NAT Translations

To view a list of NAT translations that have recently been performed and which remain in effect (for any of the defined rules), select **NAT Translations** from the NAT Options drop-down list. The NAT Translations page displays, as shown in Figure :

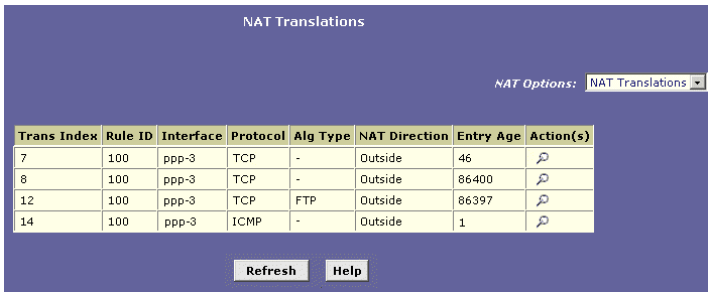

NAT Translations
NAT Options: NAT Translations
Trans Index Rule ID Interface Protocol Alg Type NAT Direction Entry Age Action(s)
7 100 ppp-3 TCP - Outside 46
8 100 ppp-3 TCP - Outside 86400
12 100 ppp-3 TCP FTP Outside 86397
14 100 ppp-3 ICMP - Outside 1
Refresh
Help

Figure 23. NAT Translations Page

For each current NAT translation session, the table contains the following fields:

Field	Description
Trans Index	The sequential number assigned to the IP session used by this NAT translation session.
Rule ID	The ID of the NAT rule invoked.
Interface	The device interface on which the NAT rule was invoked (from the rule definition).
Protocol	The IP protocol used by the data packets that are undergoing translations (from the rule definition) Example: TCP, UDP, ICMP.
Alg Type	The *Application Level Gateway* (ALG), if any, that was used to enable this NAT translation (ALGs are special settings that certain applications require in order to work while NAT is enabled).
NAT Direction	The direction (incoming or outgoing) of the translation (from the port definition).
Entry Age	The elapsed time, in seconds, of the NAT translation session.

You can click 🔍 in the Action(s) column to view additional details about a NAT translation session, as shown in Figure .

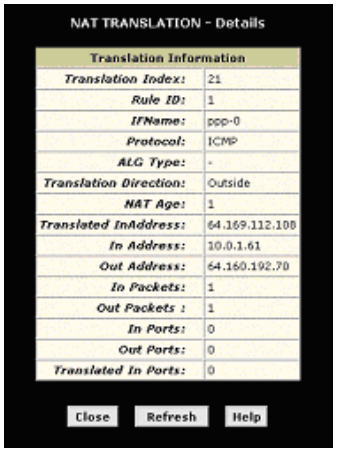


Figure 24. NAT Translation – Details Page

In addition to the information displayed in the NAT Translations table, this table displays the following for the selected current translation sessions:

Field	Description
Translated InAddress	The public IP address to which the private IP address was translated.
In Address	The private IP address that was translated.
Out Address	The IP address of the outside destination (web, ftp site, etc.)
In/Out Packets	The number of incoming and outgoing IP packets that have been translated in this translation session.
In Ports	The actual port number corresponding to the LAN computer.
Out Ports	The port number associated with the destination address.
Translated In Ports	The port number to which the LAN computer's actual port number was translated.

Adding NAT Rules

This section explains how to create rules for the various NAT flavors.

Note

You cannot edit existing NAT rules. To change a rule setup, delete it and add a new rule with the modified settings.

The napt rule: Translating between private and public IP addresses

Follow these instructions to create a rule for translating the private IP addresses on your LAN to your public IP address. This type of rule uses the NAT flavor napt, which was used in your default configuration. The napt flavor translates private source IP addresses to a single public IP address. The napt rule also translates the source port numbers to port numbers that are defined on the NAT Global Configuration page (see page 29).

Click the NAT tab, then select **NAT Rule Entry** from the NAT Options drop-down list on the right side of the page.

The NAT Rule entry page displays a row for each currently configured NAT rule.

1. Click Add to display the NAT Rule – Add page.

The NAPT flavor displays by default in the Rule Flavor drop-down list. The NAT Rule – Add page displays, as shown in Figure .

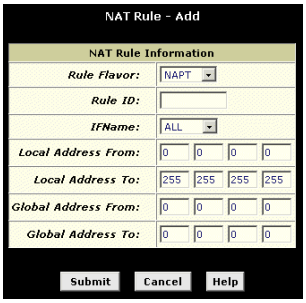


Figure 25. NAT Rule – Add Page (napt Flavor)

2. Enter a Rule ID.

   The Rule ID determines the order in which rules are invoked (the lowest numbered rule is invoked first, and so on). In some cases, two or more rules may be defined to act on the same set of IP addresses. Be sure to assign the Rule ID so that the higher priority rules are invoked before lower-priority rules. It is recommended that you select rule IDs as multiples of 5 or 10 so that, in the future, you can insert a rule between two existing rules.

   Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

3. From the IFName drop-down list, select the interface on the device to which this rule applies.

   Typically, NAT rules are used for communication between your LAN and the Internet. Because the device uses the WAN interface (which may be named *ppp-0* or *eoa-0*) to connect your LAN to your ISP, it is the usual IFName selection.

4. In the Local Address From field and Local Address To fields, type the starting and ending IP addresses, respectively, of the range of private address you want to be translated. Or, type the same address in both fields to specify a single value.

   To specify that data from all LAN addresses should be translated, type 0 (zero) in each From field and 255 in each To field.

   If you have several non-sequential private addresses, you can create an additional napt rule for each address.

   These addresses should correspond to private addresses already in use on your network (either assigned statically to your PCs, or assigned dynamically using DHCP).

5. In the Global Address From and Global Address To fields, type the public IP address assigned to you by your ISP.

   If you have multiple WAN interfaces, in both fields type the IP address of the interface to which this rule applies. This rule will not be enforced for data that arrives on other PPP interfaces.

   If you have multiple WAN interfaces and want the rule to be enforced on a range of them, type the starting and ending IP addresses of the range.

6. When you have completed entering all information, click Submit.

   A page displays to confirm the change.

7. Click Close to return to the NAT Configuration page.

   The new rule should display in the NAT Rule Configuration table.

8. Ensure that the Enable radio button is selected, and then click Submit.

   A page displays to confirm your changes.

9. Click the Admin tab, and then click **Commit and Reboot** in the task bar.

10. Click Commit to save your changes to permanent memory.

The rdr rule: Allowing external access to a LAN computer

You can create an rdr rule to make a computer on your LAN, such as a Web or FTP server, available to Internet users without requiring you to obtain a public IP address for that computer. The computer's private IP address is translated to your public IP address in all incoming and outgoing data packets.

Note

Without an rdr rule (or bimap rule described on page 39), the Best Data DSL542 blocks attempts by external computers to access your LAN computers.

Figure shows the fields used to establish a rdr rule:

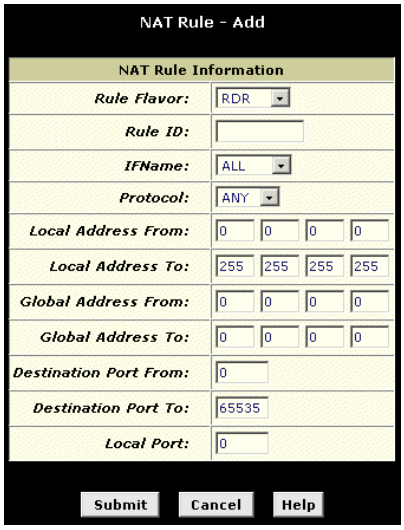


Figure 26. NAT Rule – Add Page (rdr Flavor)

Follow these instructions to add an rdr rule (see steps 1-4 under "The napt rule" on page 33 for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select **RDR** as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.

3. Select a protocol to which this rule applies, or choose **ALL**.

   This selection specifies which type of Internet communication will be subject to this translation rule. You can select ALL if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the IANA-specified protocol number.

4. In the Local Address From and Local Address To fields, type the same private IP address, or the lowest and highest addresses in a range:

   - If you type the same IP address in both fields, incoming traffic that matches the criteria you specify in steps 5 and 6 will be redirected to that IP address.
   - If you type a range of addresses, incoming traffic will be redirected to any available computer in that range. This option would typically be used for load balancing, whereby traffic is distributed among several redundant servers to help ensure efficient network performance.

   These addresses should correspond to private addresses already in use on your network (either assigned statically to your PCs or assigned dynamically using DHCP).

5. In the Global Address From and Global Address To fields, type the public IP address assigned to you by your ISP.

   If you have multiple WAN (PPP) interfaces, this rule will not be enforced for data that arrives on other PPP interfaces. This rule will not be enforced for data that arrives on WAN interfaces not specified here.

   If you have multiple WAN interfaces and want the rule to be enforced on more than one of them (or all), type the starting and ending IP addresses of the range.

6. In the Destination Port From and Destination Port To fields, enter the port ID (or a range) that you expect to see on incoming packets destined for the LAN computer for which this rule is being created.

   Incoming traffic that meets this criteria will be redirected to the Local Port number you specify in the next field.

   For example, if you grant public access to a Web server on your LAN, you would expect that incoming packets destined for that computer would contain the well-known web server port number, 80. This setting serves as a filter; data packets not containing this port number would not be granted access to you local computer.

7. If the LAN computer that you are making publicly available is configured to use a non-standard port number for the type of traffic it receives, type the non-standard port number in the Local Port field.

   This option translates the standard port number in packets destined for your LAN computer to the non-standard number you specify. For example, if your Web server uses (non-standard) port 2000, but you expect incoming data packets to refer to (standard) port 80, you would enter 2000 here and 80 in the Destination Port fields. The headers of incoming packets destined for port 80 will be modified to refer to port 2000. The packet can then be routed appropriately to the web server.

8. Follow steps 7-12 under "The napt rule" on page 33 to submit your changes.

The basic rule: Performing 1:1 translations

The basic flavor translates the private (LAN-side) IP address to a public (WAN-side) address, like napt rules. However, unlike napt rules, basic rules do not also translate the port numbers in the packet header; they are passed through untranslated. Therefore, the basic rule does not provide the same level of security as the napt rule. Figure shows the fields used for adding a basic rule.

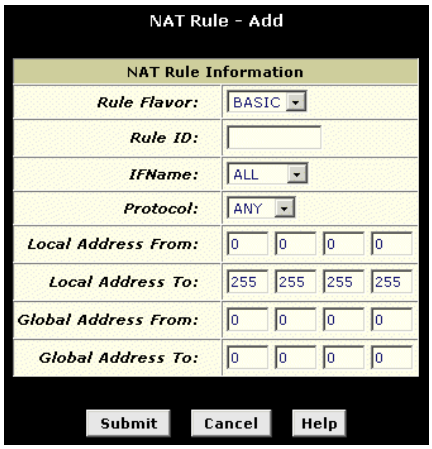


Figure 27. NAT Rule – Add Page (basic Flavor)

Follow these instructions to add an basic rule (see steps 1-4 under "The napt rule" on page 33 for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select **BASIC** as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. Select a protocol to which this rule applies, or choose **ALL**.

   This selection specifies which type of Internet communication will be subject to this translation rule. You can select ALL if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the IANA-specified protocol number.
4. In the Local Address From and Local Address To fields, type the starting and ending IP addresses that identify the range of private address you want to be translated. Or, type the same address in both fields.

   If you specify a range, each address will be translated in sequence to a corresponding address in a range of global addresses (which you specify in step 5).

   You can create a basic rule for each specific address translation to occur. The range of addresses should correspond to private addresses already in use on your network, whether assigned statically to your PCs, or assigned dynamically using DHCP.
5. In the Global Address From and Global Address To fields, type the starting and ending address that identify the pool of public IP addresses that the private addresses should be translated to. Or, type the same address in both fields (if you also specified a single address in step 4).
6. Follow steps 7-12 under "The napt rule" on page 33 to submit your changes.

The filter rule: Configuring a basic rule with additional criteria

Like the basic flavor, the filter flavor translates public and private IP addresses on a one-to-one basis. The filter flavor extends the capability of the basic rule. Refer to “The basic Rule” on page 36 for a general description.

You can use the filter rule if you want an address translation to occur only when your LAN computers initiate access to specific destinations. The destinations can be identified by their IP addresses, server type (such as FTP or Web server), or both. Figure shows the fields used to establish a filter rule.

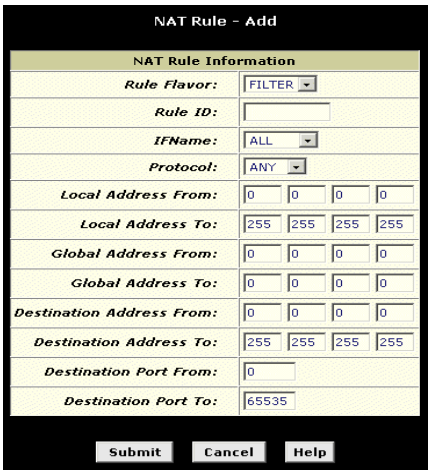


Figure 28. NAT Rule—Add Page (filter Flavor)

Follow these instructions to add a filter rule (see steps 1-4 under "The napt rule" on page 33 for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select **FILTER** as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. Select a protocol to which this rule applies, or choose **ALL**.

   This selection specifies which type of Internet communication will be subject to this translation rule. You can select ALL if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the IANA-specified protocol number.
4. In the Local Address From and Local Address To fields, type the starting and ending IP addresses that identify the range of private address you want to be translated. Or, type the same address in both fields.

   If you specify a range, each address will be translated in sequence to a corresponding address in a range of global addresses (which you specify in step 5).

   The address (or range of addresses) should correspond to a private addresses (or addresses) already in use on your network. These may be assigned statically to your PCs or assigned dynamically using DHCP.
5. In the Global Address From and Global Address To fields, type the starting and ending address that identify the range of public IP addresses to translate your private addresses to. Or, type the same address in both fields (if you also specified a single address in step 4).
6. Specify a Destination Address or addresses, Destination Port (or ports), or both. You can specify a single value by entering that value in both fields.

   - Specify a destination address (or range) if you want this rule to apply only to outbound traffic to the address (or range).

     If you enter only the network ID portion of the destination address, then the rule will apply to outbound traffic to all computers on network.
   - Specify a destination ports (or range) if you want this rule to apply to any outbound traffic to the types of servers identified by that port number.

     Port number assignments are maintained in RFCs maintained by IANA. Common port numbers include:
     20, 21—FTP (file transfer protocol) server
     25—SMTP (simple mail transfer protocol) server
     80—HTTP (World Wide Web) server

- Specify both a destination address (or range) and a destination port (or range) if you want this translation rule to apply to accesses to the specified server type at the specified IP address or network.

7. Follow steps 7-12 under "The napt rule" on page 33 to submit your changes.

The bimap rule: Performing two-way translations

Unlike the other NAT flavors, the bimap flavor performs address translations in both the outgoing and incoming directions. Figure shows the fields used to establish a bimap rule.

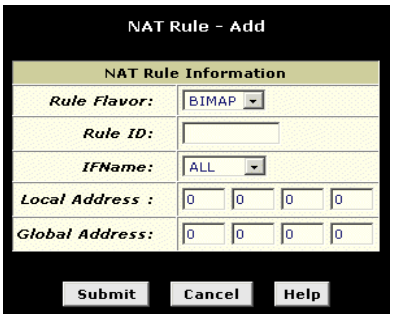


Figure 29. NAT Rule – Add Page (bimap Flavor)

Follow these instructions to add a bimap rule (see steps 1-4 under "The napt rule" on page 33 for specific instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select **BIMAP** as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. In the Local Address field, type the private IP address of the computer to which you are granting external access.
4. In the Global Address field, type the address that you want to serve as the publicly known address for the LAN computer.
5. Follow steps 7-12 under "The napt rule" on page 33 to submit your changes.

The pass rule: Allowing specific addresses to pass through untranslated

You can create a pass rule to allow a range of IP addresses to remain untranslated when another rule would otherwise do so.

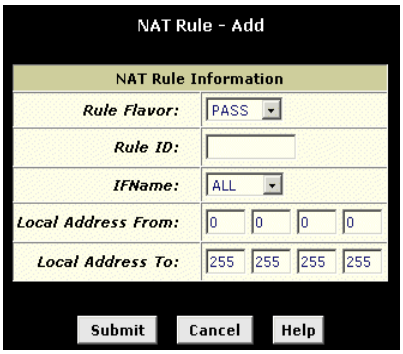


Figure 30. NAT Rule – Add Page (pass Flavor)

The pass rule must be assigned a rule ID that is a lower number than the ID assigned to the rule it is intended to pass. In you want a specific IP address or range of addresses to not be

subject to an existing rule, say rule ID #5, then you can create a pass rule with ID #1 through #4.

Follow these instructions to add a pass rule (see steps 1-4 under "The napt rule" on page 33 for detailed instructions corresponding to steps 1 and 2 below):

1. Display the NAT Rule – Add Page, select **PASS** as the Rule Flavor, and enter a Rule ID.
2. Select the interface on which this rule will be effective.
3. In the Local Address From and Local Address To fields, type the lowest and highest IP addresses that define the range of private address you want to be passed without translation.

   If you want the pass rule to act on only one address, type that address in both fields.
4. Follow steps 7-12 under "The napt rule" on page 33 to submit your changes.

8 Configuring IP Routes

You can use Configuration Manager to define specific routes for your Internet and network data. This chapter provides instructions for creating routes.

Most users do not need to define IP routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN computers and for the Best Data DSL542 provide the most appropriate path for all your Internet traffic.

- On your LAN computers, a default gateway directs all Internet traffic to the LAN port on the Best Data DSL542. Your LAN computers know their default gateway either because you assigned it to them when you modified their TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet.
- On the Best Data DSL542 itself, a default gateway is defined to direct all outbound Internet traffic to a router at your ISP. This default gateway is assigned automatically by your ISP whenever the device negotiates an Internet connection.

You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

Viewing the IP Routing Table

All IP-enabled computers and routers maintain a table of IP addresses that are commonly accessed by their users. For each of these *destination IP addresses*, the table lists the IP address of the first hop the data should take. This table is known as the device's *routing table*.

To view the Best Data DSL542's routing table, click the Routing tab. The IP Route Table displays, as shown in Figure 32.

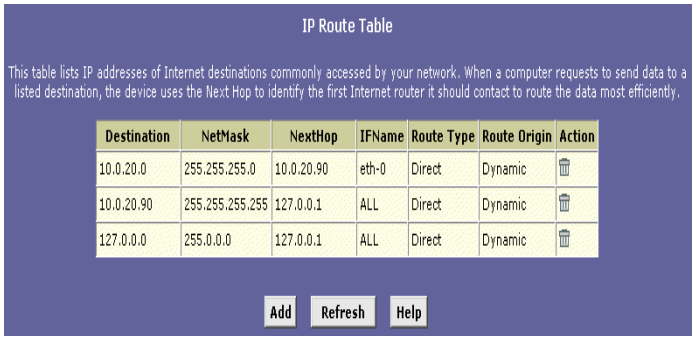


Figure 31. IP Route Table Page

The IP Route Table displays a row for each existing route. These include routes that were predefined on the device, routes you may have added, and routes that the device has identified automatically through communication with other devices.

The routing table should reflect a default gateway, which directs outbound Internet traffic to your ISP. This default gateway is shown in the row containing destination address 0.0.0.0.

The following table defines the fields in the IP Routing Table.

Field	Description
Destination	Specifies the IP address of the destination computer. The destination can specified as the IP address of a specific computer or an entire network. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Netmask	Indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. The default gateway uses a netmask of 0.0.0.0.
NextHop	Specifies the *next* IP address to send data to when its final destination is that shown in the destination column.
IFName	Displays the name of the interface on the device through which data is forwarded to the specified next hop.
Route Type	Displays whether the route is direct or indirect. In a *direct* route, the source and destination computers are on the same network, and the router attempts to directly deliver the data to the computer. In an *indirect* route, the source and destination computers are on different networks, and the router forwards data to a device on another network for further handling.
Route Origin	Displays how the route was defined. *Dynamic* indicates that the route was created automatically or predefined by your ISP or the manufacturer. Routes you create are labeled *Local*. Other routes can be created automatically (using RIP, as described in Chapter 8), or defined remotely through various network management protocols (LCL or ICMP).
Action	Displays an icon (🗑) you can click on to delete a route.

Adding IP Routes

Follow these instructions to add an IP route to the routing table.

1. From the IP Route Table page, click **Add**.

   The IP Route – Add page displays, as shown in Figure 33.

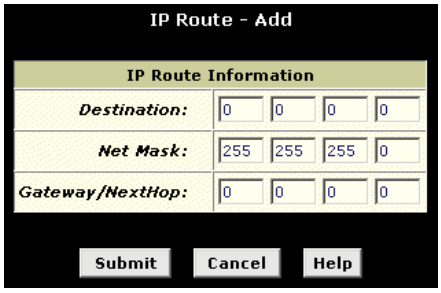


Figure 32. IP Route – Add Page

2. Specify the destination, network mask, and gateway or next hop for this route.

   To create a route that defines the default gateway for your LAN, enter 0.0.0.0 in both the Destination and Net Mask fields. Enter your ISP's IP address in the Gateway/NextHop field.

   Note that you cannot specify the interface name, route type or route origin. These parameters are used only for routes that are identified automatically as the device communicates with other routing devices. For routes you create, the routing table displays system default values in these fields.

3. Click Submit.
4. On the confirmation page, click Close to return to the IP Route table page.
   The IP Routing Table will now display the new route.
5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
6. Click Commit to save your changes to permanent memory.

9 Configuring the ATM VCC

As your LAN computers access the Internet via the Best Data DSL542, data is exchanged with your ISP through a complex network of telephone switches, Internet routers, servers, and other specialized hardware. These various devices communicate using a common language, or protocol, called *Asynchronous Transfer Mode* (ATM). On the Wide Area Network (WAN) that connects you to your ISP, the ATM protocol performs functions like those that the Ethernet protocol performs on your LAN.

This chapter describes how to configure the ATM *virtual channel connection* (VCC). The VCC properties define the path the Best Data DSL542 uses to communicate with your ISP over the ATM network.

Viewing Your ATM VC Setup

To view your current configuration, log into Configuration Manager, click the WAN tab, and then click **ATM VCC** in the task bar. The ATM VCC Configuration page displays, as shown in Figure 34.

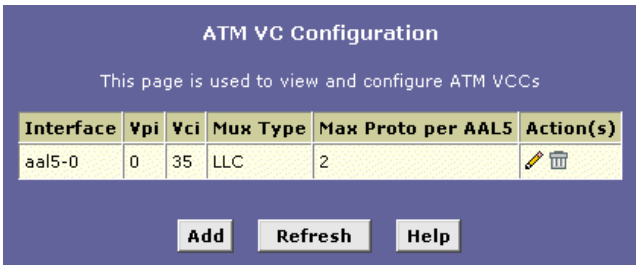


Figure 33. ATM VCC Configuration Page

The ATM VCC Configuration table displays the following fields (contact your ISP to determine these settings):

Field	Description
Interface	The name of the lower-level interface on which this VC operates. The low-level interface names are preconfigured in the software and identify the type of traffic that can be supported, such as data or voice. Internet data services typically use an AAL5-type interface.
Vpi, Vci, and Mux Type	These settings identify a unique ATM data path for communication between your ADSL/Ethernet router and your ISP.
Max Proto per AAL5	If you are using an AAL5-type of interface, this setting indicates the number of higher-level interfaces that the VC can support (the higher level interfaces can be PPP, EoA, or IPoA interfaces). Contact your ISP to determine which connection protocol(s) they require.
Actions	Displays an icon (🗑) you can click on to delete the associated interface.

Adding ATM VCCs

You may need to create a VCC if none has been predefined on your system or if you use multiple services with your ISP. Each service may require its own VCC. Follow these instructions to add a VCC:

1. From the ATM VCC Configuration page, click **Add**.

   The ATM VCC – Add page displays, as shown in Figure 35

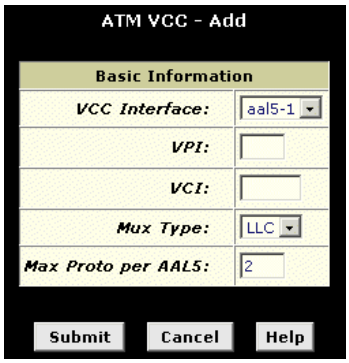


Figure 34. ATM VCC – Add Page

2. Select an interface name from the VCC Interface drop-down list.
3. Enter the VPI and VCI values assigned by your ISP, and select the mux type from the drop-down list.
4. Click **Submit**.
5. On the confirmation page, click **Close** to return to the ATM VCC Configuration page.
6. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
7. Click **Commit** to save your changes to permanent memory.

   The new interface should now display in the ATM VCC Configuration table.

You may need to create a new WAN interface, or modify an existing interface, so that it uses the new VCC. See the instructions for configuring a PPP (Chapter 10), EoA (Chapter 11), or IPoA (Chapter 12) interfaces, depending on the type you use to communicate with your ISP.

You can verify that the new settings work by attempting to access the Internet from a LAN/USB computer. Contact your ISP for troubleshooting assistance.

Modifying ATM VCCs

Your device may already be preconfigured with the necessary ATM VCC properties, or the table may contain placeholder values that you must change before using the device. Contact your ISP to determine your ATM VCC values. Follow these instructions to modify a preconfigured VCC:

1. From the ATM VCC Configuration page, click ✎ in the Actions column for the interface you want to modify.

   The ATM VCC Interface – Modify page displays, as shown in Figure 36.

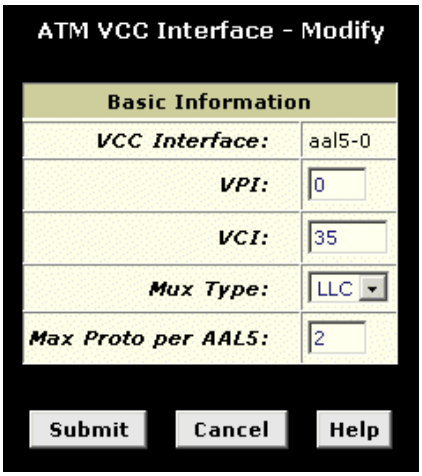


Figure 35. ATM VCC Interface – Modify Page

2. Enter the new VPI and VCI values, select the MUX type, or change the maximum number of protocols that the VCC can carry, as directed by your ISP.

   You cannot modify the interface type over which an existing VCC operates (aal5-0, for example). If you want to change the interface type, you must delete the existing interface, create a new one, and select the desired interface type.

3. Click Submit.
4. On the confirmation page, click Close to return to the ATM VCC Configuration page.
5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
6. Click Commit to save your changes to permanent memory.
7. You can verify that the new settings work by attempting to access the Internet from a LAN/USB computer. Contact your ISP for troubleshooting assistance.

10 Configuring PPP Interfaces

When powered on, the Best Data DSL542 initiates a connection through your DSL line to your ISP.

The point-to-point (PPP) protocol is commonly used between ISPs and their customers to identify and control various communication properties, including:

- Identifying the type of service the ISP provides to a given customer
- Identifying the customer to the ISP through a username and password login
- Enabling the ISP to assign Internet information to the customer's computers

Your ISP may or may not use the PPP protocol. Contact your ISP to determine if you will need to change the default settings in order to connect to their server.

Viewing Your Current PPP Configuration

To view your current PPP setup, log into Configuration Manager, click the WAN tab, and then click **PPP** in the task bar. The PPP Configuration page displays, as shown in Figure 37.

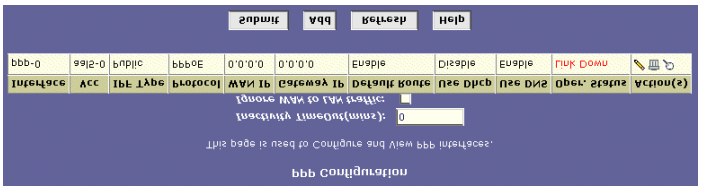


Figure 36. PPP Configuration Page

PPP is configured as a group of software settings associated with the ADSL port. Although the device has only one physical ADSL port, the Best Data DSL542 can be defined with more than one group of PPP settings. Each group of settings is called a *PPP interface* and is given a name, such as *ppp-0*, *ppp-1*, etc.

You can configure the following settings on the PPP Configuration page:

- **Inactivity TimeOut (mins)**: The time in minutes that must elapse before a PPP connection times-out due to inactivity.
- **Ignore WAN to LAN traffic**: When enabled, data traffic traveling in the incoming direction—from the WAN port to the LAN port—will not count as activity on the WAN port; i.e., it will not prevent the connection from being terminated if inactive for the specified time.

The PPP Configuration Table displays the following fields:

Field	Description
Interface	The predefined name of the PPP interface.
VCC	The Virtual Channel Connection over which this PPP data is sent. The VCC identifies the physical path the data takes to reach your ISP.
IPF Type	The type of IP Firewall protections that are in effect on the interface (public, private, or DMZ): A public interface connects to the Internet (PPP interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. A private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface -- whether from a LAN or external source -- are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness.
Protocol	The type of PPP protocol used. Your ISP may use PPP-over-Ethernet (PPoE) or PPP-over-ATM (PPoA).
WAN IP	The IP address currently assigned to your WAN (DSL) port by your ISP.
Gateway IP	The IP address of the server at your ISP that provides you access to the Internet.
Default Route	Indicates whether the ADSL/Ethernet router should use the IP address assigned to this connection as its default route. Can be Enabled or Disabled.
Use DHCP	When set to *Enable*, the device will acquire additional IP information from the ISP's DHCP server. The PPP connection itself acquires the device's IP address, mask, DNS address, and default gateway address. With Use DHCP enabled, the device will acquire IP addresses for various other server types (WINS, SMTP, POP3, etc. -- these server types are listed on the DHCP Server Configuration page).
User DNS	When set to *Enable*, the DNS address learned through the PPP connection will be distributed to clients of the device's DHCP server. This option is useful only when the ADSL/Ethernet Router is configured to act as a DHCP Server for your LAN. When set to *Disable*, LAN hosts will use the DNS address(es) preconfigured in the DHCP pool (see "Configuring DHCP Server" on page 23)
Oper. Status	Indicates whether the link is currently up or down or if a specific type of data exchange is under way (e.g., password authorization or DHCP).
Actions	You can use these icons to modify ( ), delete ( ), and view additional details on ( ) the PPP interface.

Viewing PPP Interface Details

When you click 🔍 to view additional details, the PPP Interface - Detail page displays, as shown in Figure 38

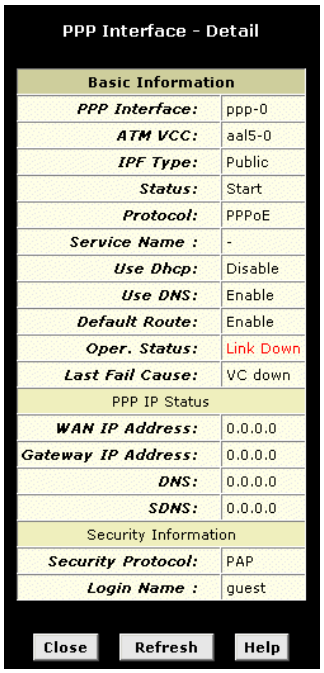


Figure 37. PPP – Detail Page

In addition to the properties defined on page 49, he Detail page displays these fields:

Field	Description
Status	Indicates whether the interface has been specified in the system as: Enabled: A connection will be established for use when the device is turned on or rebooted. Disabled: The PPP interface cannot currently be used. Start On Data: The PPP connection will be made only when data is sent to the interface (e.g., when a LAN user attempts to use the Internet).
Service Name	The name of the ISP service you are using with this PPP connection. ISPs may offer different types of services (for example, for online gaming or business communications), each requiring a different login and other connection properties.

Field	Description
Last Fail Cause	Indicates the action that ended the previous PPP session: No Valid PADO Recvd: The unit initiated a PPoE handshake but did not receive a packet in reply from the ISP. No Valid PADS Recvd: After the initial handshake, the unit did not receive a confirmation packet from the ISP. Stopped by User: The user stopped the connection (for example, by changing the Configuration Manager settings for the PPP interface.) No Activity: The PPP communication timed out, in accordance with the timeout period specified on the PPP Configuration page. Auth Failure: The ISP could not authorize the connection based on the user name and/or password provided. PADT recvd: The ISP issued a special packet type to terminate the PPP connection. VC down: The Virtual Circuit between the unit and the ISP is down. Internal failure: A system software failure occurred.
DNS	The IP address of the DNS server (located with your ISP) used on this PPP connection.
SDNS	The IP address of the secondary DNS server (located with your ISP) used on this PPP connection.
Security Protocol	The type of PPP security your ISP uses: *PAP* (Password Authentication Protocol) or *CHAP* (Challenge Handshake Authentication Protocol).
Login Name	The name you use to log in to your ISP each time this PPP connection is established.

Adding a PPP Interface Definition

If you intend to use more than one type of service from your ISP, the device may be configured with multiple PPP interfaces, each with unique logon and other properties. Follow this procedure to define properties for a PPP interface:

1. From the PPP Configuration Page, click **Add**.

   The PPP Interface – Add page displays, as shown in Figure 39.

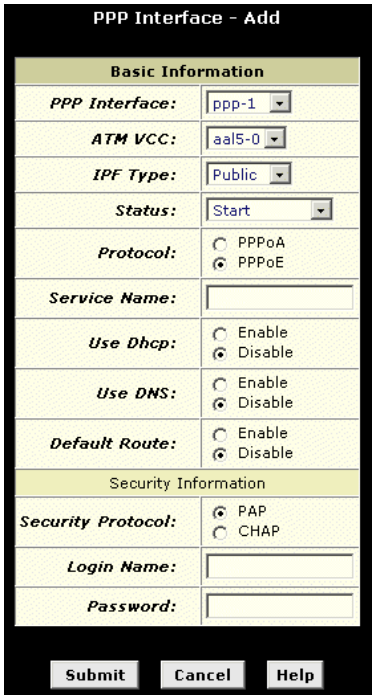


Figure 38. PPP Interface – Add Page

2. Select a PPP interface name from the drop-down list, and then enter or select data for each field.

Note

You can create multiple PPP interfaces only if you are using the PPoA protocol; only one PPP interface can be define if you are using PPoE. Check with your ISP which version of the protocol they require.

   The fields are defined in the tables on page 49 and 50.

3. Click **Submit**.

   A page displays to confirm your changes.

4. Click **Close** to return to the PPP page and view the new interface in the table.
5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
6. Click **Commit** to save your changes to permanent memory.

Modifying and Deleting PPP Interfaces

To modify a PPP interface, display the PPP Configuration page and click in the Action(s) column for the interface you want to modify. The PPP Interface – Modify page displays, as shown in Figure 40.

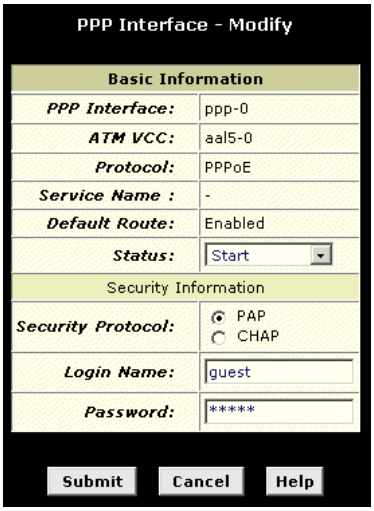


Figure 39. PPP Interface – Modify

You can change only the status of the PPP connection, the security protocol, your login name, and your password. To modify the other settings, you must delete the interface and create a new one.

To delete a PPP interface, display the PPP Configuration page and click in the Action(s) column for the interface you want to delete. You should not delete a PPP interface unless you have received instructions to do so from your ISP. Without an appropriately defined PPP interface, you will not be able to connect to your ISP. You can recreate the PPP interface with the same name at a later time.

After modifying or deleting a PPP interface, click Submit. Then, Click the Admin tab, click **Commit & Reboot** in the task bar, and click Commit to save your changes to permanent memory.

11 Configuring EOA Interfaces

This chapter describes how to configure an Ethernet-over-ATM interface on the Best Data DSL542, if one is needed to communicate with your ISP.

Viewing Your EOA Setup

To view your current EOA configuration, log into Configuration Manager, click **Advanced** in the task bar, and then click **EOA**. Figure 41 shows the EOA configuration page.

Figure 40. EOA Page

The EOA table contains a row for each EOA interface currently defined on the device. The table may contain no entries if your ISP does not use the EOA protocol.

The following table describes the fields on this page:

Field	Description
Interface	The name the software uses to identify the EOA interface.
IPF Type	The type of IP Firewall protections in effect on the interface (public, private, or DMZ): A *public* interface connects to the Internet (IPoA interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. A *private* interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. The term *DMZ* (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface—whether from a LAN or external source—are subject to a level of protection that is in between those for public and private interfaces.
Lower interface	EOA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port —the WAN port). This field should reflect an interface name defined in the next lower level of software over which the EOA interface will operate. This will be an ATM VCC interface, such as *aal5-0.*

Field	Description
Config IP Address and Net Mask	The IP address and network mask you want to assign to the interface. If the interface will be used for bridging with your ISP and you will not be using the Best Data DSL542 as a router on your LAN, then you do not need to specify IP information. If you enable DHCP for this interface, then the Configured IP address will serve only as a request to the DHCP server. The actual address that is assigned by the ISP may differ if this address is not available.
Use DHCP	When checked, this setting instructs the device to accept IP information assigned dynamically by your ISP's DHCP server. If the interface will be used for bridging with your ISP and you will not be routing data through it, leave this checkbox unselected.
Default Route	Indicates whether the Best Data DSL542 should use the IP address assigned to this interface, if any, as its default route for your LAN. This can be *Enable* or *Disable*. See Chapter 8 for an explanation of default routes.
Status	A green or red ball will display to indicate that the interface is currently up or down, respectively. You cannot manually enable or disable the interface; a red ball may indicate a problem with the DSL connection.
Action	Icons you can click on to edit ( ) or delete ( ) the associated EOA interface.

Adding EOA Interfaces

Follow these instructions to add an EOA interface:

1. Click the WAN tab, and then click **EOA** in the task bar.
2. Click Add.

The EOA Interface – Add page displays, as shown in Figure 42.

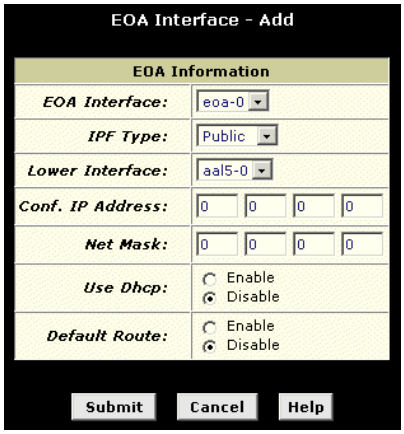


Figure 41. EOA Interface – Add Page

3. Select one of the predefined interface names from the EOA Interface drop down list.
4. From the IPF Type drop-down list, select the level of IP Firewall to be used on this interface, as defined above.

5. In the Lower Interface field, select the lower-level interface name over which this protocol is being configured. Typically, an EOA interface is configured to operate over an aal5 interface, such as *aal5-0*.

If you are using the Best Data DSL542 as a bridge only, skip to step 7.

6. If you are using the Best Data DSL542 as a router on your LAN, enter the IP address and network mask you want to assign to the interface. This address serves as the public IP address for your entire LAN and is usually assigned by your ISP.

   Or, if your ISP will assign this information, click the Enable radio button to set up the DHCP service.

   Also, specify whether this interface should serve as the default route for your LAN for accessing the Internet.

7. Click Submit.

   A confirmation page display to confirm your changes.

8. Click Close to return to the EOA page and view the new interface in the table.
9. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
10. Click Commit to save your changes to permanent memory.

12 Configuring IPoA Interfaces

This chapter describes how to configure an IPoA (Internet Protocol-over-ATM) interface on the Best Data DSL542.

Viewing Your IPoA Interface Setup

To configure an IPoA interface, log into Configuration Manager, click the WAN tab, and then click **IPoA** in the task bar. The IPoA page displays, as shown in Figure 43.

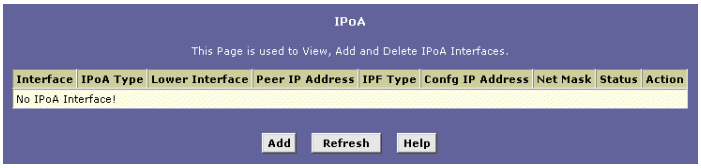


Figure 42. IPoA Page

The IPoA table contains a row for each EOA interface currently defined on the device. The table may initially contain no entries.

The following table describes the fields on this page:

Field	Description
Interface	The name the software uses to identify the IPoA interface
IPoA Type	Specifies whether or not the IPoA protocol to be used complies with the IEFT RFC 1577 "Classical IP and ARP over ATM" (contact your ISP if unsure).
Lower interface	IPoA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port – the WAN port). This field should reflect an interface name defined in the next lower level of software over which the IPoA interface will operate. This will be an ATM VCC interface, such as *aal5-0*.
Peer IP Address	The IP address of the remote computer you will be connecting to via the WAN interface.

Field	Description
IPF Type	The type of IP Firewall protections that are in effect on the interface (public, private, or DMZ): A *public* interface connects to the Internet (IPoA interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. A *private* interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. The term *DMZ* (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets incoming on a DMZ interface—whether from a LAN or external source—are subject to a level of protection that is in between those for public and private interfaces.
Config IP Address and Net Mask	The IP address and network mask you want to assign to the interface.
Status	A green or red ball will display to indicate that the interface is currently up or down, respectively. You cannot manually enable or disable the interface; a down interface may indicate a problem with the DSL connection.
Action	Icons you can click on to edit ( ) or delete ( ) the associated EOA interface.

Adding IPoA Interfaces

Follow these instructions to add an IPoA interface:

1. Display the IPoA page and click **Add**.

   The IPoA Interface – Add page displays, as shown in Figure 44.

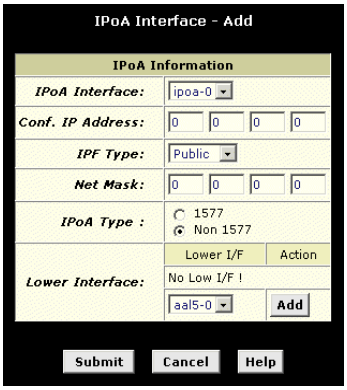


Figure 43. IPoA Interface – Add Page

2. Select the next available interface name from the IPoA Interface drop-down list.
3. In the Configured IP Address and Net Mask boxes, type the address and mask that you want to assign to the IPoA interface.

4. Select the level of firewall security to apply to the interface by selecting the IPF Type as Public, Private, or DMZ.
5. In the Lower Interface dialog box, select the lower-level interface name over which this protocol is being configured and click **Add**. Typically, an IPoA interface is configured to operate over an aal5 interface.
6. Click **Submit**.

   A confirmation page will display to confirm your changes.
7. Click **Close** to return to the EOA page and view the new interface in the table.
8. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
9. Click **Commit** to save your changes to permanent memory.

13 Configuring Bridging

The Best Data DSL542 can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN. This chapter describes how to configure the Best Data DSL542 to operate as a bridge.

Note

Before changing your bridge configuration, check with your ISP to determine the type of connection they use to exchange data with their customer's DSL modems (such as Ethernet bridging or IP routing).

Using the Bridging Feature

Although the Best Data DSL542 is preconfigured to serve as a router for providing Internet connectivity to you LAN, there are several instances in which you may also want to configure bridging:

- Your ISP may use protocols that require bridging with your LAN. The device can be configured to appear as a bridge when communicating with your ISP, while continuing to provide router functionality for your LAN.
- Your LAN may include computers that communicate using "layer-3" protocols other than the Internet Protocol. These include IPX® and AppleTalk®. In this case, the device can be configured to act as a bridge for packets that use these protocols while continuing to serve as a router for IP data.

In both cases, you need to specify the device's interfaces as bridge interfaces.

Defining Bridge Interfaces

To enable bridging, you simply specify the device interfaces on which you want to bridge data, and then enable bridging mode:

1. Log into Configuration Manager and click the Bridging tab.

   The Bridge Configuration page displays, as shown in Figure 45.

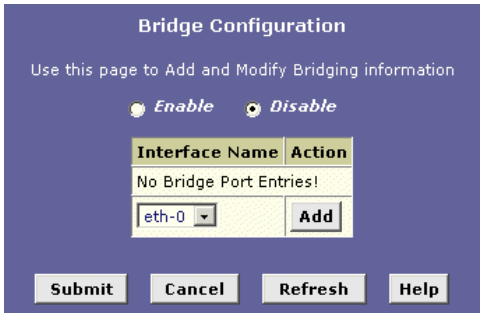


Figure 44. Bridge Configuration page

   The table may be empty if bridging has not yet been configured.

2. Select the interface names on which you want to perform bridging and click **Add**.

   For example, select *eth-0* (LAN) and *eoa-0* (WAN) interfaces. If you use such protocols on a USB-connected computer, you can also select *usb-0*.

Note

You have to create an entry for usb-0 inferface via RS-232 cable. Please refer the procedure on page 10 and type "create bridge port intf ifname usb-0" on step 7.

If you do not have an eoa-0 interface, but instead have an interface named ppp-0 *or* ipoa-0*, your device is not currently configured with a WAN interface that allows bridging with your ISP. You may want to check with your ISP to determine whether they use the eoa protocol. See Chapter 11 for instructions on creating an EOA interface.*

Note

If you enable bridging on an interface that has already been assigned an IP address, then it is considered IP-enabled and will route (rather than bridge) IP packets received on the interface. The interface will bridge non-IP data it receives, however.

You can determine whether the Ethernet (eth-0) and USB (usb-0) interfaces have been assigned IP addresses by displaying the IP Address Table (display the Routing tab, and then click **IP Address***). These interfaces will display in the table only if they have been assigned IP addresses.*

You can check whether the eoa-0 interface has been assigned an IP address by displaying the EOA configuration table (click the WAN tab, and then click **EOA***). If the Config IP Address field is empty and the Use DHCP field contains the word Disable, then no IP address has been assigned.*

3. Click the **Enable** radio button to turn on bridging.
4. Click Submit.

   A page will briefly display to confirm your changes, and will return you to the Bridge Configuration page.
5. Click the Admin tab, and then click **Commit & Reboot** in the task bar.
6. Click Commit to save your changes to permanent memory.

Deleting a Bridge Interface

1. To make an interface non-bridgeable, display the Bridge Configuration page and click 🗑 next to the interface you want to delete. Click OK to confirm the deletion. The interface remains defined in the system, but is no longer capable of performing bridging.

A Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the Best Data DSL542, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

Problem	Troubleshooting Suggestion
LEDs	
Power LED does not illuminate after product is turned on.	Verify that you are using the power cable provided with the device and that it is securely connected to the Best Data DSL542 and a wall socket/power strip.
LINK WAN LED does not illuminate after phone cable is attached.	Verify that a standard telephone cable like the one provided is securely connected to the ADSL port and your wall phone jack. Wait 30 seconds to allow the device to negotiate a connection with your ISP.
LINK LAN LED does not illuminate after Ethernet cable is attached.	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the Best Data DSL542. Make sure the PC and/or hub is turned on. Verify that you are using a straight-through type Ethernet cable to the uplink port on a hub or a cross-over type cable to a stand-alone PC. If you connected the device to an ordinary hub port (not Uplink), you must use a straight-through cable. (Hold the connectors at each end of the cable side-by-side in the same position. If the order of their color-coded wire pairs is the same, it is a straight-through type.) Contact Customer Support if your cable is not the correct type. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled Cat 5. 10Mbit/sec cables may tolerate lower quality cables.
Internet Access	
PC cannot access Internet	Use the ping utility, discussed in the following section, to check whether your PC can communicate with the Best Data DSL542's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: Check that the gateway IP address on the computer is your public IP address. If it is not, correct the address or configure the PC to receive IP information automatically. Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically. Verify that a Network Address Translation rule has been defined on the Best Data DSL542 to translate the private address to your public IP address. The assigned IP address must be within the range specified in the NAT rules (see Chapter 7). Or, configure the PC to accept an address assigned by another device. The default configuration includes a NAT rule for all dynamically assigned addresses within a predefined pool (see the instructions in Chapter 6 to view the address pool).
PCs cannot display web pages on the Internet.	Verify that the DNS server specified on the PCs is correct for your ISP, as discussed in the item above. You can use the ping utility, discussed in the following section, to test connectivity with your ISP's DNS server.

Problem	Troubleshooting Suggestion
Configuration Manager Program	
You forgot/lost your Configuration Manager user ID or password.	If you have not changed the password from the default, try using "root" as both the user ID and password. Otherwise, you can reset the device to the default configuration by pressing the Reset button on the back panel of the device (using a pointed object such as a pen tip). Then, type the default User ID and password shown above. **WARNING:** Resetting the device removes any custom settings and returns all settings to their default values.
Cannot access the Configuration Manager program from your browser.	Use the ping utility, discussed in the following section, to check whether your PC can communicate with the Best Data DSL542's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer v5.0 or later, or Netscape Navigator v4.7 or later. Support for Javascript® must be enabled in your browser. Support for Java® may also be required. Verify that the PC's IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the Best Data DSL542.
Changes to Configuration Manager are not being retained.	Be sure to use the Commit function after any changes. This function is described on page 17.

Diagnosing Problem using IP Utilities

ping

Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer you are trying to communicate with.

On Windows-based computers, you can execute a ping command from the Start menu. Click the Start button, and then click Run. In the Open text box, type a statement such as the following:

ping 192.168.1.1

Click OK. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

If the target computer receives the message, a Command Prompt window displays like that shown in Figure .

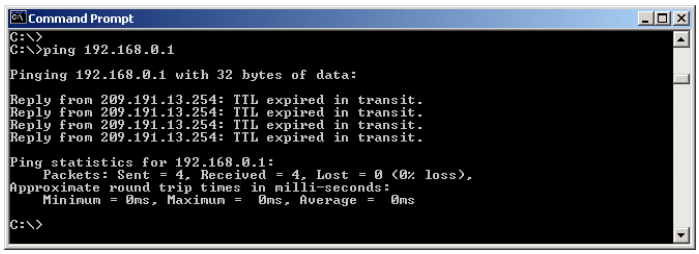

Command Prompt
C:\>
C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 209.191.13.254: TTL expired in transit.
Reply from 209.191.13.254: TTL expired in transit.
Reply from 209.191.13.254: TTL expired in transit.
Reply from 209.191.13.254: TTL expired in transit.
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>

Figure 45. Using the ping Utility

If the target computer cannot be located, you will receive the message "Request timed out."

Using the ping command, you can test whether the path to the Best Data DSL542 is working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for www.yahoo.com (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the nslookup command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

nslookup

You can use the nslookup command to determine the IP address associated with an internet site name. You specify the common name, and the nslookup command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the nslookup command from the Start menu. Click the Start button, and then click Run. In the Open text box, type the following:

nslookup

Click OK. A Command Prompt window displays with a bracket prompt (>). At the prompt, type the name of the internet address your are interested in, such as www.microsoft.com.

The window will display the associate IP address, if known, as shown in Figure 1.

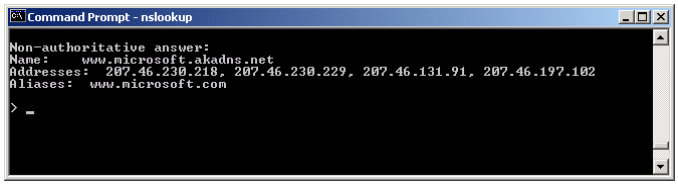


Figure 1. Using the nslookup Utility

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the nslookup utility, type **exit** and press **<Enter>** at the command prompt.